AIZPILDA PATENTU VALDE

SAŅEMŠANAS Nr.	SAŅEMŠANAS DATUMS

LATVIJAS REPUBLIKAS
PATENTU VALDEI
Citadeles iela 7/70
Rīga, LV–1010
Latvija
Tālr.: +371 67099600
Fakss: +371 67099650

IESNIEGUMS
PATENTA
PIEŠĶIRŠANAI

PATENT
APPLICATION

PIETEICĒJA ŠIFRS **[** 33093 **]**

LŪDZU PIEŠĶIRT PATENTU ŠĀDAM IZGUDROJUMAM

54 Izgudrojuma nosaukums

IERĪCE UN METODE SAPULCES DALĪBNIEKU BIOMETRISKAI IDENTIFIKĀCIJAI, SAPULCES IERAKSTA VEIKŠANAI UN KOPSAVILKUMA ĢENERĒŠANAI

Izgudrojuma nosaukums angliski

DEVICE AND METHOD FOR BIOMETRIC IDENTIFICATION OF MEETING PARTICIPANTS, MEETING RECORDING AND SUMMARY GENERATION

71 PIETEICĒJS/PIETEICĒJi (PAREDZAMAIS PATENTA ĪPAŠNIEKS/ĪPAŠNIEKI)	ADRESE, VALSTS
BIOMETRIC WITNESS SIA	Ieriķu 58-189 Rīga, LV-1084 Latvija

□ PIETEICĒJS IR ARĪ IZGUDROTĀJS
□ PIETEICĒJS IR SKOLĒNS, STUDENTS, PENSIONĀRS VAI PERSONA, KURAI PIEŠĶIRTA I VAI II INVALIDITĀTES GRUPA

72 IZGUDROTĀJS/IZGUDROTĀJI (VĀRDS, UZVĀRDS)	ADRESE, VALSTS
Aleksejs Bankovskis	Ieriķu 58-189 Rīga, LV-1084 Latvija

□ IZGUDROTĀJS ATTEICIES NO TIESĪBĀM TIKT MINĒTAM VAI PIEPRASĪJIS, LAI VIŅŠ NETIKTU MINĒTS

74 PĀRSTĀVIS	ADRESE
Anna Timofejeva AAA LAW LATVIA	Citadeles iela 12 Rīga, LV-1010 Latvija

70 ADRESE SARAKSTEI
Anna Timofejeva

NOSAUKUMS
AAA LAW LATVIA

ADRESE
Citadeles iela 12
Rīga, LV-1010, Latvija

ADRESĀTA VEIDS Fiziska persona

PERSONAS KODS

E-PASTS anna@aaalaw.lv

TĀLRUNIS 67324695

KOMUNIKĀCIJAS UN DOKUMENTU SAŅEMŠANAS VEIDS

PATENTA REĢISTRĀCIJAS APLIECĪBAS VEIDS E-apliecība

PATENTMEKLEJUMS

☒ Lūdzu veikt patentmeklējumu
☒ Apliecinu ka esmu mazais vai vidējais uzņēmums

PIELIKUMI:

Apraksts (neskaitot gēnu sekvences sarakstu un ar tām saistītas tabulas) - 33093_Description_ENG.pdf
Zīmējumi - 33093_Drawings_ENG.pdf
Pretenzijas - 33093_Claims_ENG.pdf
Kopsavilkums - 33093_Abstract_ENG.pdf

IESNIEDZĒJA DATI

VĀRDS, UZVĀRDS / NOSAUKUMS Anna Timofejeva
AIZPILDĪŠANAS DATUMS 13.12.2024

PIETEIKUMS PATENTA PIEŠĶIRŠANAI

APLIECINĀJUMS PAR PATENTA PIETEIKUMA IESNIEGŠANU

Jūsu patenta pieteikums tika iesniegts veiksmīgi. Paldies, ka izvēlējāties pieteikt patentu Latvijā, izmantojot tiešsaistes pieteikuma formu.

Pieteikuma detaļas

E-pieteikuma pagaidu numurs	EPLV202400000063027	
Iesniegšanas datums	13.12.2024	
Iesniegšanas laiks	18:53	
Pielikumu skaits	4	
Apmaksas statuss	Samaksāts	
Maksājums:		
	Pieteikuma maksa	120,00 EUR
	Maksājuma kopsumma	120,00 EUR

JA PATENTS TIKS ATZĪTS PAR REĢISTRĒJAMU, PAR REĢISTRĀCIJU UN PUBLIKĀCIJU BŪS JĀMAKSĀ REĢISTRĀCIJAS MAKSA.

DEVICE AND METHOD FOR BIOMETRIC IDENTIFICATION OF MEETING PARTICIPANTS, MEETING RECORDING AND SUMMARY GENERATION
DESCRIPTION

Field of the invention

[001] The present invention relates to a portable meeting device with biometric identification of participants and its operating method.

Background of the invention

[002] US patent US9064160B2 discloses an arrangement and corresponding method, which arrangement is configured to recognize a conference participant who is currently talking during a conference session. The arrangement comprises an identifying unit including a biometric detector adapted to capture at least one biometric characteristic of the participant and a comparison unit adapted to compare the biometric characteristic to stored biometric characteristics in a database each stored characteristic being associated with an owner identity.

[003] US patent application US2019190908A1 discloses a system for managing an access control a meeting. The system may include a communication interface that receives video and audio of the meeting, a processor that executes instructions to generate a biometric characteristic for an attendee based on at least one of the video and the audio, and to associate identity information of the attendee with the biometric characteristic based on a comparison of the biometric characteristic with stored biometric characteristics of known users. The processor may also execute the instructions to generate a data stream that includes at least one of the video and the audio of the attendee, to tag the data stream with the identity information based on the associated biometric characteristic, and to selectively cause the data stream to be shown on a display based on selection of the tag.

[004] US patent US11315366B2 discloses a method of obtaining a multimedia file corresponding to a conference, the multimedia file includes video data and audio data. Personal identity information of each person is identified according to the facial features and the voice features of each person. Once the audio data corresponding to each person is converted into text information, the posture language, the personal identity information, and the text information corresponding to each person are output.

[005] The present invention provides an alternative improved way of meeting participation control and meeting overview generation.

Summary of the invention

[006] The present invention generally refers to a device and method for authorizing, initializing, conducting, and recording meetings, using biometrics technology for participant identification. It is an object of the present invention to provide an advanced meeting device and an associated method designed to improve the security, accuracy, and accountability of meetings by authenticating participants through their biometric data.

[007] The meeting device described in the present application includes: a camera on each side of the device, a microphone on each side of the device, a central processing unit (CPU), a fingerprint scanner, a RFID reader, a memory card and a USB-C port. The device is capable of an advanced biometric authentication via combination of results of a facial recognition and a fingerprint scanning to securely verify participants' identities. The device allows for automated generation of detailed meeting minutes, derived from recorded audio and video data, based on machine intelligence, therefore, capturing essential contributions and decisions made during the meeting.

[008] A method described in the present application includes: capturing image information by the camera and biometric information by the fingerprint scanner about the participant joining the meeting; identifying or verifying participants identity by comparing the information retrieved with the one stored in the database; verification of the results in order to grant or deny access to the meeting. The method further includes a user-initiated meeting documentation step, where the activated cameras and microphones of the meeting device capture video and audio of the meeting. The data collected are stored in the system's memory and subsequently utilized to create an overview of the meeting. Furthermore, the video received from cameras is stitched for seamless panoramic view of the meeting, and the audio received from the microphones is transcripted and summarized by machine intelligence into meetings minutes.

Brief description of the drawings

[009] The drawings illustrate generally, by way of the example, but not by way of limitation, various embodiments of the invention.

[010] Fig. 1 is a process flowchart of the meeting device.

[011] Fig. 2 is a connectivity framework of the meeting device.

[012] Fig. 3 is an operational overview of the meeting device.

[013] Fig. 4 is a flowchart of participant verification method step implemented by the device.

[014] Fig. 5 is a flowchart of meeting documentation method step implemented by the device.

Detailed description of the invention

[015] The present invention provides a meeting support device and with it associated implementing method. By utilizing advanced biometric authentication - such as facial recognition and fingerprint scanning - the system ensures that only authorized individuals gain access to confidential discussions and sensitive information, thereby mitigating the risk of unauthorized attendance. In conjunction with video and audio capture, this technology creates a comprehensive and accurate record of the meeting, including contributions and interactions from all participants. Such innovative approach improves the effectiveness of meetings. Through automatic recording and minute generation, the device enhances transparency, providing an accurate record that can be referenced for follow-up actions and accountability. Reliable framework allows users to maintain a consistent meeting history, aiding in decision-making and reinforcing security standards. Ultimately, the combination of biometric identification, simultaneous various data capture, and intelligent summarization significantly elevates the meeting experience, making it more efficient, secure, and productive.

[016] Meeting room device can include, by way of example and not limitation, a number of different components including meeting software and portable meeting hardware. The present invention encompasses meeting hardware designed to facilitate the execution of meetings in accordance with the features described herein. This hardware may include, but is not limited to, CPU, at least one integrated wide-angle lens camera with the frame rate of at least 60 frames per second (FPS) for smooth video recording, positioned on each side of the device, which can be selectively activated or deactivated based on specific requirements for video capture and facial recognition, or depending on necessity of its use. Additionally, the meeting hardware incorporates at least one built-in omnidirectional microphone array with sensitivity at least about -40 dBV/Pa for audio capture and at least one fingerprint scanner to further enhance functionality. The fingerprint scanner has a resolution of at least 500 DPI. The disclosed device operates on a rechargeable battery, enabling autonomous functionality and efficient data recording through the use of a SDXC memory card of class 10 or higher with UHS-I or UHS-II support. To enhance security of the information disclosed during meetings a robust encryption for all data is provided, ensuring its secure storage and transmission. Additionally, the device supports integration with

multi-standard RFID readers supporting a wide range of RFID standards, such as HF and UHF frequencies, to enhance access control capabilities, and includes a USB-C port for charging and data transfer, providing versatility and ease of use in various operational environments. The USB-C port is in a direct connection to a power management system and CPU of the meeting device. This combination of features ensures that the device is not only user-oriented but also prioritizes security and reliability in data management.

[017] The interaction of the components can be divided into 5 main steps as seen in components interaction flowchart of Fig. 1. The steps are as follows:

Initialization: the system powers on and initiates a self-check to ensure all components are operational. During this phase, the CPU engages all connected peripherals, including the cameras, microphones, fingerprint scanner, and RFID reader, preparing them for subsequent data capture.

Data capture: once initialization is complete, the cameras and omnidirectional microphones commence capturing video and audio data from the meeting environment. This ensures that all participants are clearly visible and audible. Meanwhile, the fingerprint scanner and RFID reader remain in standby mode, ready to activate when participant identification is required.

Data processing: the captured audio and video data is sent to the CPU for processing. The CPU employs algorithms to stitch the images captured by the cameras, creating a comprehensive panoramic view. Simultaneously, biometric processing occurs, utilizing facial recognition and fingerprint scanning to authenticate participants. This multi-faceted processing ensures accurate representation and verification of all attendees.

Data storage: following processing, the system encrypts the data to protect sensitive information during storage and transmission. The encrypted data is then securely stored on the memory card, facilitating efficient retrieval while maintaining compliance with data privacy regulations.

User interaction: finally, users can access the stored data through web or mobile interfaces, allowing for easy review and management of meeting content. This feature enhances user experience by providing flexibility in accessing meeting minutes, video recordings, and audio files, all from a convenient platform.

[018] The hardware of the meeting device operates in conjunction with software of the meeting device to enable various meeting-related functions, such as participant identification, initiation of meetings, audio and video recording, and further generation of meeting minutes. Moreover, the system allows for generation of a footage of the meeting, irrespectively of the positioning of the participants during the meeting, contributing to a more dynamic and efficient post-meeting experience.

[019] The present invention discloses the meeting support device that integrates multiple functionalities through a connectivity framework as seen in Fig. 2 accordingly.

[020] The components of the device are interconnected as further described. The device comprises four wide-angle lens cameras, each positioned on a different side of the unit. The cameras are interfaced with the CPU via high-speed serial connections, utilizing protocols such as MIPI (Mobile Industry Processor Interface) or USB. Each camera can be individually activated or deactivated as per the requirements of the meeting. An integration of four omnidirectional microphones is a key feature of the device, facilitating the capture of audio from all directions. Each microphone is connected to the CPU through either digital or analog interfaces, specifically I2S (Inter-IC Sound) or PDM (Pulse Density Modulation). A fingerprint scanner is incorporated into the device, connecting to the CPU via a serial interface such as UART, I2C or SPI. An inclusion of the multi-standard RFID reader, connected to the CPU via a serial connection (UART or I2C), allows for efficient access management. This feature streamlines the identification process of participants using RFID tags. The device is equipped with an SDXC memory card slot that interfaces with the CPU via the SD or SDIO interface. This functionality permits the storage of various data types, including recorded audio, video, and meeting documentation, facilitating easy retrieval and management of meeting records. A USB-C port serves as a dual-purpose connection point, linking both the power management system and the CPU. This port supports data transfer and charging capabilities, providing versatility for connectivity with other devices.

[021] Fig. 3 is an operational overview of the meeting device that illustrates the comprehensive functionality of the same, highlighting its capabilities in data capture, processing, storage, and user interaction.

[022] Flowcharts shown in Figs. 4-5 depict exemplary methods of operation for various embodiments of the present invention. To improve clarity, these flowcharts highlight certain steps while omitting others that would be evident to those skilled in the art. As such, the flowcharts should not be interpreted as mandating all the illustrated steps or excluding any unillustrated steps. Additionally, the sequence of steps presented is not fixed, as many steps can be performed independently of one another.

[023] Fig 5. illustrates a method of identity verification having a first step of initiation of identity verification by a user. The meeting device initializes cameras in from of each participant which captures an image of the participant’s face and processes features like the distance between eyes, nose, mouth, and other unique facial attributes. At the same time, the system initializes the fingerprint scanner to scan the individual's fingerprint. Data obtained by both the camera and the

fingerprint scanner are sent to the system. The system further performs a step of comparison of obtained data with pre-stored biometric characteristics of the participant. The CPU retrieves pre-stored matching biometric data from the memory of the device or database. In turn, for captured data, both the facial recognition score and fingerprint matching score are evaluated. The system combines these two scores to make a final determination about whether the person is authentic or not. The algorithm used for such multi-modal biometric fusion combines the results from both the facial recognition and fingerprint matching. This process involves techniques like weighted summation and machine learning models. The results from facial and fingerprint matching are assigned weights (importance), and the scores from both modalities are summed up. If the combined score exceeds a certain threshold, when compared with the pre-stored biometric data, the identity is verified. Machine learning models utilized provide how the scores from different modalities are to be combined for a precise result. This process increases the reliability of identity verification, reducing the chances of false positives (incorrectly verifying an individual) or false negatives (incorrectly denying access). The facial recognition technology employs Convolutional Neural Networks (CNNs), with models like FaceNet chosen for their accuracy in variable lighting and facial angles, frequently encountered in meeting settings. For fingerprint identification minutiae-based algorithms are utilized to identify key features, such as ridge endings and bifurcations, to create a precise match between the captured fingerprint and stored templates. The fingerprint scanners utilize UART, I2C, or SPI, for interfacing with advanced software libraries, such as Neurotechnology's VeriFinger SDK, therefore, providing robust tools for accurate, fast, and secure fingerprint identification. Together, these modalities provide a robust and reliable access control system, implemented using OpenCV with TensorFlow or PyTorch frameworks for facial recognition and VeriFinger SDK for fingerprint matching. To implement multi-modal biometric fusion, BioAPI and OpenBR software platforms and frameworks are used to support the different authentication modalities and facilitate the combination of biometric data. Data encryption is fundamental for safeguarding sensitive biometric information during both processing and storage. The encryption process uses AES 256-bit encryption, a robust standard that protects against unauthorized access. Key management follows stringent protocols, with options to integrate Hardware Security Modules (HSM) to securely generate, store, and manage encryption keys. For further security, Public Key Infrastructure (PKI) standards are implemented to protect key exchange and digital signature processes, ensuring that only authorized devices and personnel can access the stored data. This multilayered security framework provides comprehensive data protection, ensuring confidentiality and compliance with data privacy regulations. After the step of data comparison, the system verifies the identity of the participant or marks the participant as unrecognized and further an explicit consent from other recognized participants must be received for such participant to be allowed to attend the meeting.

[024] Fig. 6 is a flowchart of yet another exemplary procedure of the disclosed method for obtaining event documentation and minutes of the meeting. The procedure has a first step of initiation of the event documentation by a user. Then the system activates and records video and audio by means of four cameras and four omnidirectional microphones. The recorded video and audio data are further sent to the system and stored in the memory of the meeting device. The stored video and audio data are further processed by the system to obtain 360-degree video with synchronized audio. The 360-degree image is obtained by a stitching process that aligns and blends overlapping areas from multiple video frames captured simultaneously by the device's cameras, creating a continuous 360-degree view. The stitching algorithms, including SIFT (Scale-Invariant Feature Transform) and SURF (Speeded-Up Robust Features), detect distinctive key points within each frame, matching them across images for precise alignment. After alignment, multi-band blending techniques are applied to eliminate visible seams, resulting in a seamless panoramic view suitable for fully capturing meetings. This process is optimized for closed environments like conference rooms where overlapping visuals are essential for context. This is particularly useful for environments requiring 360-degree visual coverage, such as in the context of meeting room devices with multiple cameras. Technologically, the process is implemented but not limited to using libraries like OpenCV, which includes dedicated stitching modules. These modules provide the necessary tools for feature detection, image alignment, and blending, or alternatively, specialized software solutions can be utilized for more complex stitching requirements. This technology enhances the visual continuity of multi-camera systems, offering comprehensive and unified video output for applications like meeting recordings and surveillance.

[025] The present invention includes precise audio synchronization with captured video, ensuring cohesive alignment of multimedia data. The input for this synchronization process consists of timestamped audio data from multiple microphones and corresponding video frames. Digital Signal Processing (DSP) algorithms process these timestamps, aligning the audio and video to eliminate any discrepancies. This synchronization improves clarity and coherence, enabling accurate playback and documentation of recorded content. Technologies such as beamforming for directional focus and noise reduction methods like Wiener filtering further enhance audio quality, isolating speaker voices from background noise for a more polished output. The technology that supports audio synchronization includes DSP processors and software libraries

like PortAudio or PyAudio, which provide the necessary tools for real-time audio processing and synchronization. By ensuring that audio and video are seamlessly aligned, above-mentioned feature greatly enhances the user experience in applications such as video conferencing, event recording, and multimedia production, leading to more engaging and professional-quality content.

[026] As one of the essential features of the present invention is considered to be speech transcription to written text. The software on a meeting room device enables a meeting minutes to be generated and to be sent to the attendees. The meeting minutes include a timeline of events that took place during the meeting and, additionally, the content discussed throughout the meeting. In operation, when a meeting begins, the meeting room device, through its meeting software, automatically monitors and records events occurring during the meeting, generating a timeline of these events. An addition of a geotag is possible. The generation of meeting minutes is intricately linked to the processes of image stitching and audio synchronization. Video images captured from multiple cameras are stitched together to create a cohesive visual representation of the meeting, which is then synchronized with audio data collected from various microphones. Leveraging artificial intelligence, the system can intelligently generate meeting minutes by identifying the standard introductory and concluding phrases, which are used for ensuring a coherent and organized summary of the discussions held during the meeting. This combined approach of synchronized audio and video enhances the accuracy and comprehensiveness of the meeting documentation.

[027] While the invention may be susceptible to various modifications and alternative forms, specific embodiments of which have been shown by way of example in the figures and have been described in detail herein, it should be understood that the invention is not intended to be limited to the particular forms disclosed. Rather, the invention includes all modifications, equivalents, and alternatives falling within the scope of the invention as defined by the following claims.

CLAIMS

1. A meeting device comprising:

a body of the meeting device,

at least one microphone on each side of the meeting device adapted to capture audio of meeting participants,

at least one camera on each side of the meeting device adapted to capture video of the meeting participants, wherein each camera is deactivated when not in use,

a fingerprint scanner arranged on one side of the meeting device,

an RFID reader,

a memory card,

a central processing unit (CPU) in communication with said at least one microphone on each side of the meeting device, at least one camera on each side of the meeting device, fingerprint scanner, RFID reader and memory card,

wherein the CPU being configured to execute the computer-executable instructions to generate a visual biometric characteristic of the participant based on the image of a video stream captured; generate a biometric characteristic of the participant based on a fingerprint pattern captured by the fingerprint scanner; retrieve pre-stored matching biometric data from a memory of the device and send to the CPU; perform multi-modal biometric fusion of said generated biometric characteristics; compare the obtained data with a pre-stored participant's identity; verify identity of the participant or mark the participant as unrecognised; based on the verification, allow or deny the participant an access to the meeting, wherein in case an access to the meeting is denied the CPU is being configured to request a permission for access from identified participants of the meeting,

wherein the CPU executes the computer-executable instructions to detect key points in images or video frames of the video stream captured from each of said cameras; align said images or video frames and blend transitions between said images or video frames to obtain panoramic video stream of the meeting; synchronize audio captured by each of said microphones based on timing of video frames of said video captured;

wherein the CPU executes the computer-executable instructions to monitor and record events; generate a timeline of the same; generate minutes of the meeting by converting the audio captured into text information, wherein the text is generated using a machine intelligence, extracting key information of the meeting.

2. A method of identification of meeting participants, meeting recording and meeting summary generation, comprising:

generating a visual biometric characteristic of the participant based on the image of a video stream captured; generating a biometric characteristic of the participant based on a fingerprint pattern captured by the fingerprint scanner; retrieving pre-stored matching biometric data from a memory of the device and sending to the CPU; performing multi-modal biometric fusion of said generated biometric characteristics; comparing the obtained data with a pre-stored participant's identity; verifying identity of the participant or marking the participant as unrecognised; allowing or denying the participant an access to the meeting, wherein in case an access to the meeting is denied the CPU is being configured to request a permission for access from identified participants of the meeting;

wherein the method further including detecting key points in images or video frames of the video stream captured from each of said cameras; aligning said images or video frames and blending transitions between said images or video frames to obtain panoramic video stream of the meeting; synchronizing audio captured by each of said microphones based on timing of video frames of said video captured;

wherein the method further including monitoring and recording events; generating a timeline of the same; generating minutes of the meeting by converting the audio captured into text information, wherein the text is generated using a machine intelligence, extracting key information of the meeting.

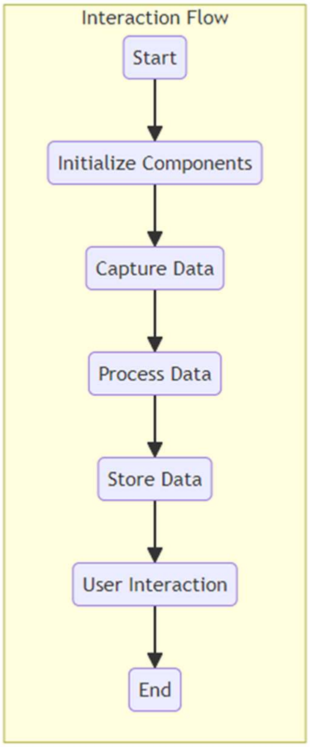
Interaction Flow
Start
Initialize Components
Capture Data
Process Data
Store Data
User Interaction
End

Fig. 1

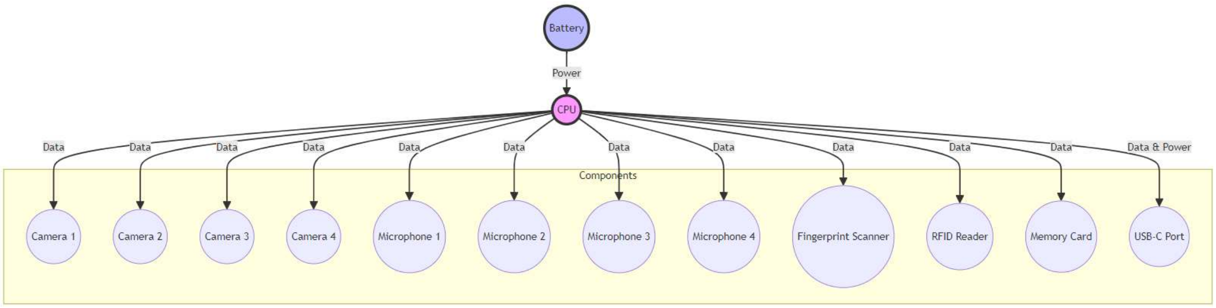
Battery
Power
CPU
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data & Power
Components
Camera 1
Camera 2
Camera 3
Camera 4
Microphone 1
Microphone 2
Microphone 3
Microphone 4
Fingerprint Scanner
RFID Reader
Memory Card
USB-C Port

Fig. 2

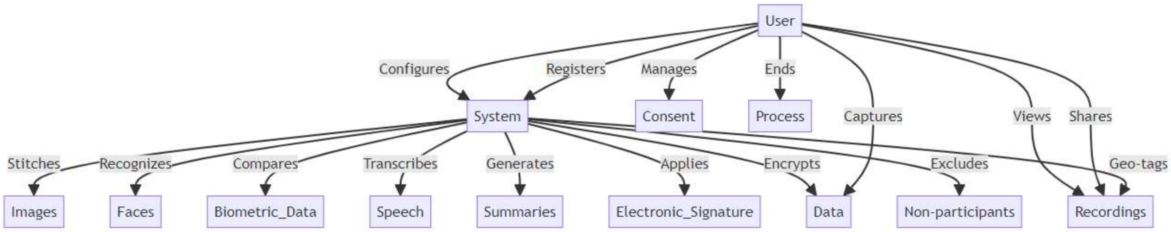
User
Configures
Registers
Manages
Ends
System
Consent
Process
Captures
Views
Shares
Stitches
Recognizes
Compares
Transcribes
Generates
Applies
Encrypts
Excludes
Geo-tags
Images
Faces
Biometric_Data
Speech
Summaries
Electronic_Signature
Data
Non-participants
Recordings

Fig. 3

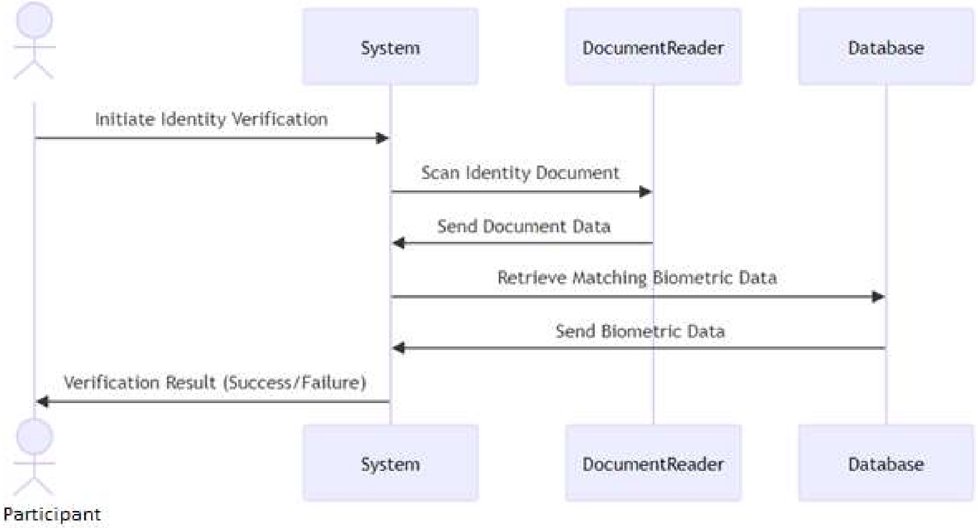
System
DocumentReader
Database
Initiate Identity Verification
Scan Identity Document
Send Document Data
Retrieve Matching Biometric Data
Send Biometric Data
Verification Result (Success/Failure)
System
DocumentReader
Database
Participant

Fig. 4

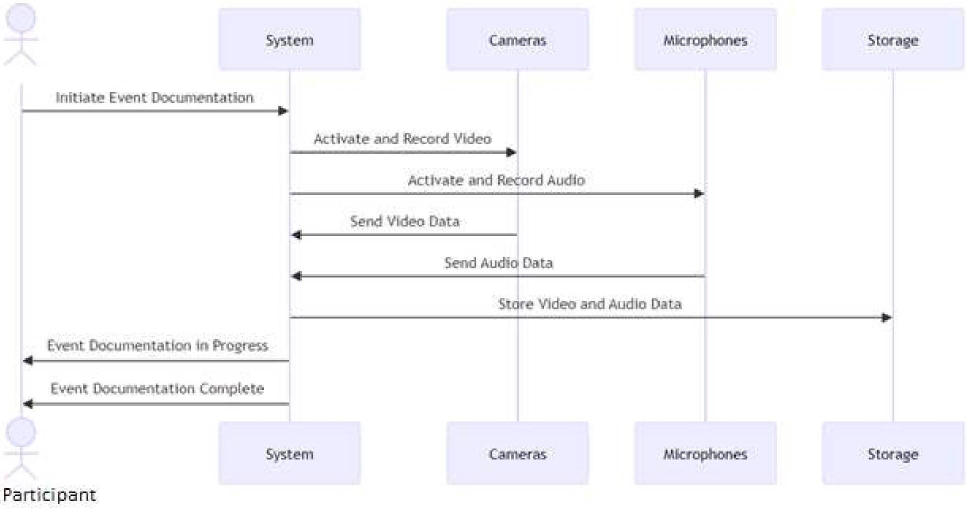
System
Cameras
Microphones
Storage
Initiate Event Documentation
Activate and Record Video
Activate and Record Audio
Send Video Data
Send Audio Data
Store Video and Audio Data
Event Documentation in Progress
Event Documentation Complete
System
Cameras
Microphones
Storage
Participant

Fig. 5

ABSTRACT

The present invention refers to a device and a method for authorizing, initializing, conducting, and recording meetings, using advanced biometrics technology for participant identification. The device comprises at least one camera on each side of the device, a microphone on each side of the device, a fingerprint scanner, a central processing unit that execute instructions to generate a biometric characteristic of the participant based on data captured by said cameras, microphones, and a fingerprint scanner. Multi-modal biometric fusion is utilized for identification of a participant. The system performs a comparison of fused captured data with a pre-stored data retrieved from the database and, if the match is found, the system grants to the participant the access to the meeting. The central processing unit may also execute instructions to generate minutes of the meeting and obtain a 360° view of the meeting with aligned audio and video streams via image stitching and audio synchronization.