DYNAMIC USER AUTHENTICATION

Government License Rights

The United States Government may have certain rights in some aspects of the invention claimed herein, as the invention was made with United States Government support under award / contract number DASG60-01-C-0054 issued by the Space Missile Defense Command, SMDC of Huntsville, Alabama.

Abstract

A system for authenticating a user for access to a remote secure system or database is accomplished by combining the recording of the transcript of the access with biometric identifiers of accessors while prompting of the accessors to perform unanticipated "surprise" tasks. The surprise element in the invention as well as the recorded transcript of the access work together to discourage and prevent identity theft and improve the likelihood of the apprehension of identity thieves.

Technical Field:

The present invention is for authenticating users remotely while discouraging and preventing identity theft.

Background:

There exists an ever increasing need to identify, or authenticate, humans. This need arises in a wide variety of applications, such as security, user access, electronic commerce, personal customization, remote controls, and the like. Three types of user authentication exist in the

art. The first type of authentication is based on something the user knows, such as a password, PIN, or personal information including a social security number or mother's maiden name. The second type of authentication is based on something the user has, such as a card key, smart card, token, or the like. The third type of authentication is more recent and is based on a biometric characteristic unique to the user, such as a fingerprint, iris scan, retina scan, or set of facial features.

One need for authentication is to battle the increasing occurrences of identity theft. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. The personal data may include elements of user authentication, such as Social Security numbers, bank account or credit card numbers, telephone calling card numbers, and the like.

Biometric verification of the current art generally fits into two broad categories: the physiological, which uses static physical characteristic, and the behavioral, which matches the dynamics of some consistently performed actions, such as saying one's name or penning one's signature. The present invention is aiming to define additional categories while at the same time broadening the definition of the two categories and blurring the distinction between them at the same time. Currently, products based on static physiological measurements are by far the most common-with finger, palm, hand geometry, face, iris and retina recognition being the most mature technologies. Researchers have proposed many other approaches, including ear geometry, vein structure and even body odor. On the other hand, behavioral biometric verifiers so far proposed are voice and handwriting recognition.

Interest in biometric user authentication has been growing based on the belief that biometric identifiers, such as fingerprints or iris scans, are unique to a single person and cannot be stolen and thus are immune to identity theft. However, experience has shown that using simple and static biometric authentication can not and will not prevent identity theft. Just as the acquisition of personal information, passwords, PINs and social security numbers have taken place, such as when such information is wrongfully obtained by breaking into computers or intercepting communication over an unsecured channel, or simply found on a

discarded piece of paper, biometric information, too can fall easily into the wrong hands. For instance, someone can take a fingerprint without the knowledge of an authorized user and use it to obtain access.

In fact, with biometric identifiers being used for authentication there is an added issue: Unlike passwords that can be changed, biometric identifiers can not be changed, e.g., your fingerprint can not be reset whereas a stolen password can. Behavioral biometric identification attempts to alleviate the problem somewhat, but falls short of offering a complete identity theft proof solution.

Another possible limited solution is to encrypt authentication data. Encryption has been used to prevent unauthorized acquisition of private information, including user authentication information. Extensive research and engineering has been, and continues to be devoted to encryption. However, encryption often requires complex algorithms and requires the use of keys which may become lost or stolen. Further, the field of encryption has been subject to government regulation and restriction. Also, note that encryption is not even relevant when someone lifts a fingerprint from a wine glass. Thus, encryption may not solve the problem for all applications.

What is needed is the ability to render identity theft pointless. The present invention achieves improved verification through dynamic authentication.

Summary of the Invention

It is a primary objective of the present invention to provide procedures that discourage identity theft as well as render identity theft pointless. This implies that not only the identity criteria changes constantly so that a set of information which allowed access at one time will be useless for gaining access the next time but also the committers of the identity theft crime have a higher risk of being apprehended.

There are three parts to the invention, and these are:

1- Obtaining a transcript of the access to make sure that a real person willing to be recorded is trying to gain access,

2- Presenting the accessor with an element of surprise asking him or her to produce a new unanticipated evidence of his or her identity at each access attempt by prompting the accessor to perform a new task or new set of tasks, and

3- Dynamic biometric verification of the accessor to assure that (a) the accessor indeed performed the task prompted in (2) and the information the accessor provided uniquely identifies him or her sufficiently to authenticate the accessor.

Brief Description of the Drawings

Figure 1. Dynamic user authentication flowchart

Figure 2. Accessor trying to gain access to a remote secure system

Figure 3. An audio visual transcript of access being sent to the remote secure server

Figure 4. An audio element of surprise

Figure 5. A visual element of surprise

Figure 6. An element of surprise using the fingerprint sensor

Figure 7. An element of surprise using handwriting recognition

Figure 8. An element of surprise using retinal or iris recognition and eye movements

Figure 9. An audio based dynamic biometric verification

Figure 10. A visual speech analysis process for matching observed mouth shapes with expected mouth shapes for the articulation of the phrase

Figure 11. A visual dynamic biometric verification process combining visual speech analysis with face recognition

Figure 12. A dynamic biometric verification process using the fingerprint sensor

Figure 13. A dynamic biometric verification process using handwriting recognition

Figure 14. A dynamic biometric verification process using retinal or iris recognition and eye movement tracking

Figure 15. Iris recognition where camera on the access device captures a picture of the user's eye, in particular iris

Figure 16. Accessor/user is prompted to mark his or her lips and eyes with a stylus

Figure 17. Face recognition is performed on the accessor/user's facial photo

Figure 18. Accessor/user is prompted with a random phrase and the camera on the PDA captures the video and the microphone on the PDA captures the audio transcript of the event

Figure 19. Audio and video signals are synchronized and the locations of lips in the captured frames are marked. One can then process this information in a manner similar to that shown in Figure 10.

Figure 20.Voice authentication compares the signal from the audio transcript to the known voiceprint of the user/accessor

Figure 21.A decision is made about the series of analysis depicted in Figures 15-20 above regarding the authenticity of the user.

Figure 22. Further assessments can be performed using the audio visual transcript including mental alertness emotional state and sincerity of the user/accessor

Figure 23. Summary sample audio visual dynamic user authentication process

Detailed Description of the Preferred Embodiments

User authentication process should (1) make it easier for law enforcement to apprehend identity theft criminals, (2) contain one or more steps that render identity theft pointless, and (3) uniquely establish the accessor as the person he or she claims to be. Three elements of the present invention itemized above, namely obtaining a transcript of the access, an element of surprise, and biometric identification under Summary of the Invention are intended for these three purposes.

These three elements that constitute the dynamic user authentication process of this invention as depicted in flowchart form in **Error! Reference source not found.** will now be described in detail.

1. Obtaining a transcript of the access:

A person who walks into a bank or walks up to an ATM and engages in a fraudulent transaction risks being identified and apprehended later on, either by being recognized by a human bank teller or by being recorded by an ATM video camera. A similar system can be put in place for persons who are accessing remote secure systems to engage in various transactions via computer, cellular phone, personal digital assistant or other devices. Such an access is depicted in Figure 2.

An audio or visual or audio visual transcript of the accessor's session is a simple non-intrusive and natural means to keep a record of the transaction. An audio transcript can be recorded by a microphone and a visual transcript can be recorded by a camera. Many devices used to access remote secure systems, such as computers, cellular phones, personal digital assistants, are already equipped with microphones and cameras that can record these transcripts and present them to the remote secure server to which the accessor trying to gain access. This is depicted in Figure 3.

Such a transcript available for later identification will severely discourage criminals from attempting the crime of fraudulent access. The transcript can also be checked to ascertain if any disguises have been put on – such as a mask.

Furthermore, this transcript, e.g., an audio visual recording of the access, can later provide the means for both the surprise element and the biometric identifier.

2. Presenting the accessor with an element of surprise

The element of surprise aims to change the identity criteria in an unanticipated manner so that a set of information which allowed access at one time will be useless for gaining access in the future. The use of changing authentication criteria is what is being referred to as "the element of surprise."

Existing static biometric identification processes simply verify that the biometric information provided by the user matches the one on file. Dynamic authentication verifies that there is a live user (i.e., the accessor) willing to subject himself or herself to scrutiny attempting to gain access to a secure remote system and during this authentication process also verifies a unique set of biometric criteria provided by that person.

In dynamic authentication, the user is asked to produce new evidence of identity each time authentication is sought. This means that the user cannot get in twice simply by presenting the same biometric information, such as a fingerprint, twice. Moreover, the user cannot gain authorization by stealing an authorized fingerprint, copying it somehow, editing it somewhat and re-presenting the edited fingerprint. In dynamic authentication, the user is asked to supply at least one randomly selected aspect of his or her identity each time identification is required. This aspect is not known to the accessor prior to access. The accessor has a few seconds to produce it. The selected aspect should still be "unique" to the accessor, like biometric identity elements used in static methods.

In the first preferred embodiment depicted in flowchart form in Figure 4 this surprise element, dynamic authentication uses audio input only. This can be accomplished by a microphone recoding the accessor while he or she is talking after the accessor is prompted to speak a random phrase. This phrase is not known to the accessor beforehand. This randomness of the phrase provides the desired element of surprise. Each time access is requested, the accessor is prompted to speak a new phrase. Therefore, stealing or intercepting the previous authentication response is counterproductive. The remote secure system initially has to verify that the accessor actually spoke the prompted phrase. This is accomplished by sending the audio signal detected by the microphone to a speech recognition engine. The speech recognition engine then verifies that the spoken phrase matches the prompted phrase. Furthermore, the remote secure system has to verify that the voice patterns recorded match those of the accessor.

In the second preferred embodiment depicted in flowchart form in Figure 5, the user speaks the phrase while a camera captures his or her face and lip movements. The remote secure system, as was the case in the previous preferred embodiment, first verifies that the phrase articulated by the lips matches the one prompted. The video signal recorded by the camera is sent to an audiovisual speech recognition engine which verifies that lip movements articulated by the user match the prompted phrase. Furthermore, the remote secure system also verifies that the facial features match the ones on file for the accessor.

One can combine the first and the second preferred embodiments towards audio visual dynamic user authentication. This combination constitutes a non-intrusive and natural way to dynamically authenticate users. This process is actually very similar to the authentication process the accessor would go through during a human-to-human transaction, e.g., at a bank teller. Notice that there are no fingerprints, no retinal or iris scans which many people would find intrusive or offensive.

In the third preferred embodiment, dynamic user authentication uses fingerprint sensors. The accessor is asked to scan one or more of his or her fingers. The remote secure system then has to verify that indeed the prompted finger(print)s made the correct prompted movements on the fingerprint scanning device and that the fingerprints thus captured do

indeed belong to the accessor. For example, the accessor is asked to scan his or her left thumb left to right on the fingerprint scanning device. The digits and the prompted motions are not known a priori to the user. The remote secure system then has to verify that indeed the correct digits (fingers) made the correct prompted movements on the fingerprint scanning device. The concept is illustrated pictorially in Figure 6.

In the fourth preferred embodiment, dynamic user authentication uses handwriting recognition. One potential element of surprise could be that the accessor gets prompted with a new random phrase which he needs to write on a pressure sensitive pad using his finger, or a writing instrument, such as a stylus. The remote secure system then has to verify that the accessor indeed penned the prompted phrase and that particular manner in which the accessor penned the script is consistent with his or her writing style. The concept is illustrated in Figure 7.

In the fifth preferred embodiment, dynamic user authentication uses iris recognition or retinal scan combined with eye tracking. For example, the accessor can be asked to track a moving arrow with his or her gaze. The remote secure system then has to verify that the retinal scan or the pattern of the iris matches the accessor's stored information and that the eyes moved in the correct manner consistent with the prompted movements of the arrow on the screen. The concept is illustrated in Figure 8.

3. Dynamic biometric verification of the accessor

Dynamic user authentication described thus far combines transcripting of the accessor's attempted access to the remote secure system – whether such transcript is recorded via audio or visual or audiovisual or other sensors and means – with the element of surprise by asking the accessor to perform an act or a series of acts which are difficult or impossible to anticipate by the accessor prior to engaging in the access process.

One can think about the recording of the performance of the prompted act or acts as another transcript itself.

The third element of the present invention analyses the transcript of the accessor's response to the prompted act or acts to verify first that indeed the performed act or acts match the prompted, and second that the transcript indeed matches the biometric data expected from the accessor.

This third and very important element of the invention is described for each of the five preferred embodiments below:

In the first preferred embodiment, the audio recording made by the microphone following the prompting of the accessor is transmitted to the remote secure server. The audio recording is analyzed by an automatic audio speech recognition processor. This processor translates the audio speech signal to text. The recognized text is compared with the prompted text and if there is a match, the audio recording is further analyzed by a voice recognition processor. The voice recognition processor compares the audio recording with the previous voice print obtained from the accessor. If the voiceprint of the current recording matches the known voice characteristics of the accessor, access is authorized. Note that the speech recognition (i.e., the dynamic verification) and voice recognition (i.e., the biometric verification) can proceed in parallel. However, as a practical matter, usually speech recognition comes before voice recognition. Each of the two processes can have various levels of confidence and associated thresholds. Moreover various methods can be employed for combining the evidence from the two processes. The process is illustrated in Figure 9.

In the second preferred embodiment, the video recording made by the camera following the prompting of the accessor is transmitted to the remote secure server. There the video recording is analyzed by an automatic visual speech analysis and/or recognition processor. A visual speech analysis processor studies the video image to determine and/or characterize the observed mouth shapes and their attributes and compare them to those anticipated given the prompted phrase (and thus the expected sequence of mouth shapes). Mouth shapes that correspond to speech elements are called visemes. The visual speech analysis processor has embedded in it previously determined models for mouth shapes from which it first produces a model for the prompted phrase consisting of a series of visemes. The visual speech

analysis processor then compares the sequence mouth shapes observed in the video recording to that model to produce a measure of how good the match is. The generally preferred techniques in the art for such analysis include Hidden Markov Models for model generation, maximum likelihood analysis and various Bayesian statistical and inference methods for measuring the likelihood of a match.

To illustrate this concept with a simple example, consider that the prompted phrase is the word "one" which phonetically can be represented as "wan." Referring to Figure 10, the left column shows the model corresponding to the expected viseme sequence of the way "one" is articulated. This model can be a generic (an average model for all speakers of the language) or a specific (restricted model given the gender or facial features of the accessor subject) or custom (trained specifically using the accessor's way of articulating speech with his or her lips) model. The right column on the other hand shows the observed sequence of mouth shapes obtained by analysis of the video recording recorded while the accessor is articulating the prompted phrase. The visual speech analysis processor compares the two columns for determining the likelihood of match or correspondence. One obvious extension of this type of analysis for more robust operation is using multiple models and base the match decision on multiple streams of evidence.

Alternately, one can use a visual speech recognition processor. In that case, the processor translates the visual speech signal to text. The visual speech signal, as before, is defined by the shapes the mouth of the accessor takes while articulating the prompted phrase, as well as various attributes characteristics or features of the mouth and the shapes the mouth assumes. As was the case with the audio based dynamic biometric verification of the first preferred embodiment, the recognized text is compared with the prompted text to see if there is a match. Visual speech recognition is a difficult task due to the ambiguousness of the viseme-phoneme correspondence. A visual speech recognizer which operates in a reliable manner is not yet available commercially – whereas many audio speech recognizers are.

Thus far, we have only described the dynamic verification of the second preferred embodiment. One obvious biometric verifier for the second preferred embodiment, as is depicted in Figure 11 is face recognition. Face recognition can come before or after the

visual speech analysis and/or recognition process, or occur simultaneously with it. The face recognition processor compares the frames of the face in the video recording with the previous face photo or model obtained from the accessor. If the features of the face in the current video recording match the known facial features and characteristics of the accessor, access is authorized. Off-the-shelf packages that can be integrated to this process exist, such as the Face-It Verification SDK from Identix for face recognition and Voice Verifier from Nuance.

In the third preferred embodiment a fingerprint sensor is used dynamically to authenticate the accessor. The process is illustrated in Figure 12. Initially, the accessor is prompted to scan one of his or her fingers in a particular direction across the fingerprint sensor. The accessor does not know which finger or which direction. The sensor takes multiple snapshots of the finger as it moves across the sensor. The data is transmitted to the remote secure server. The remote secure server verifies that (1) the data from the fingerprint sensor is consistent with the prompted movement, and (2) the fingerprint is of the correct digit of the accessor.

Current state of the art in fingerprint recognition usually progresses like this: First a gray scale fingerprint image often undergoes binarization, followed by thinning, in the preprocessing stage, in order to extract the minutia points. The recognition process is usually based on minutiae matching. Minutiae are local discontinuities in terms of terminations and bifurcations of the ridge lines that constitute a fingerprint pattern. The dynamic user authentication system described would use the same process for biometric verification, but would take multiple snapshots or frames of the fingerprint as it moves across the sensor and extract minutiae of each frame. The minutiae in each frame would be used to determine the movement across the sensor to verify that indeed the finger performed the prompted motion.

In the fourth preferred embodiment a handwriting recognition system is used dynamically to prompt the accessor to type a specific phrase and verify that the accessor actual penned the prompted phrase and the manner in which he or she penned it matches the expected manner

in which the accessor writes. Signatures are already used as a biometric in a static manner. Moreover, the idea of using handwriting or signature dynamics to authenticate signatures is not new, either. For several years, I.B.M. sold a system based on the principle to banks and other financial institutions to authorize computer transfers of large amounts of money. But such systems use costly, specially made pens and require the transfer of relatively large amounts of data, making them impractical for retailers with thousands of cash registers. Given that forgers of signatures move their pen in a far more controlled manner and can not reproduce the cadence of the movement of the true authentic signatory, and the widespread use of personal digital assistants with pressure sensitive screens, it seems, a cheaper simpler systems that dynamically verify signatures should emerge in the near future. The fourth preferred embodiment of this invention, on the other hand, takes dynamic user verification based on handwriting further by adding the surprise element, i.e., by prompting the accessor to script an unanticipated phrase each time, instead of his or her signature. The process is illustrated as a flowchart in Figure 13.

In the fifth preferred embodiment of the present invention, a retinal or iris recognition system is used in cooperation with an eye tracking process. Both retinal and iris scans are well established biometrics already in use. Retinal scanning analyses the layer of blood vessels at the back of the eye. Scanning involves using a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. It does require the user to remove glasses, place their eye close to the device, and focus on a certain point. Iris scans analyze the features that exist in the colored tissue surrounding the pupil which has more than 200 points that can be used for comparison, including rings, furrows and freckles. The scans use a regular video camera style and can be done from further away than a retinal scan.

The accessor is asked to follow a cursor on the screen with his or her eyes. The camera on the device from which the accessor is attempting to access the remote secure server (i.e., access device) takes multiple pictures of the accessor performing this prompted task. The video sequence thus captured is transmitted to the remote secure server and analyzed. This analysis involves eye tracking or gaze determination or both. Eye tracking leads to the

determination of the direction of gaze, which in turn determines the user's current line of sight or point of fixation. The fixation point is defined as the intersection of the line of sight with the surface of the object (such as the screen) being viewed. Both eye tracking and gaze are active areas of research and several techniques exist in the art. If this analysis reveals that the accessor did indeed make the eye movements required and/or his or her direction of gaze matched the one anticipated, then the dynamic part of the verification is complete. The user may then be prompted for a retinal or an iris scan. Alternately, the retinal or iris scan can come before the dynamic verification or be done simultaneously with it as the accessor is following the moving arrow or the cursor on the screen.

The fifth preferred embodiment of this invention, takes based on retinal or iris scans further by adding the surprise element, i.e., by prompting the accessor to follow a cursor or an icon on the screen which moves in an unanticipated manner. Thus, theft of iris or retinal patterns is not useful for breaking into a secure remote server. The process is illustrated as a flowchart in Figure 14.

Sample Audio Visual Dynamic User Authentication Process:

The sample dynamic authentication process outlined is basically a combination of the preferred embodiment one and two outlined above. The dynamic user authentication process can simply verify voiceprint and facial features without additional biometric information being required. Yet, many applications may require a more thorough verification of a user's biometric characteristics, the dynamic authentication can also involve alternate or additional biometric identification elements. In the sample step by step process explained below, a static iris scan is added to the dynamic authentication procedure.

Moreover, the sample process does not have an explicit audio visual transcripting up front. Instead, it embeds the audio visual transcripting within the dynamic biometric verification.

The video and the audio data provided are used for both recording the accessor's transaction and also for voiceprint and facial feature matching.

Figures 15-22 present schematic diagrams illustrating operation of an embodiment of this sample process based on the present invention are shown. This embodiment combines iris recognition with audiovisual speech recognition, voice authentication, and face recognition.

As will be recognized by one of ordinary skill in the art, other combinations of characteristics fall within the spirit and scope of the present invention. Also, the order of various identification steps may be readily modified. Further, particular biometric criteria required for authentication may be varied in keeping with the dynamic aspect of the present invention.

The example illustrated used a personal digital assistant (PDA) to capture audio and visual samples and to provide visual feedback to the user. Any form of input capture and output presentation may be used such as, for example, one or more of a personal computer, a telecommunications device, a home entertainment device, a digital camera, a microphone, an infrared sensor, a medical scanner, a fingerprint scanner, an audio speaker, a monitor, or the like.

Referring now to Figure 15, iris recognition is provided. A camera on the PDA takes a picture of the user's eye. This may be accomplished by prompting the user to move relative to the PDA until the user's eye appears to fill a box on the PDA screen. The user then presses a button or provides a verbal command and the PDA captures a picture of the retina. A computer program, either within the PDA or running on a separate computer such as a remote secure server in communication with the PDA, extracts features of the iris and compares these features against similar stored features. Note that this static method can easily be fooled by using a photograph of the retina of an authorized user.

Referring now to Figures 16 and 17, facial feature recognition is provided. In this authentication example, the user is next asked to provide a full-face image on the PDA. Once taken, the user is prompted to mark the top, bottom, left and right extent of her lips and

to mark the center of her eyes. These markings assist in facial feature recognition which, in this example, are based on the relative location of the eyes, nose and mouth to the outline of the face as well as on the shape of the face. Once again, this static method can easily be fooled by using a photograph of the face of an authorized user. However, the combined use of two static tests, selected from many that are possible, greatly reduces the chance for success for identity thieves.

Referring now to Figures 18 and 19, the user is prompted to speak a randomly generated phrase. While keeping a full-face image on the PDA screen, the user is asked to say this random phrase. This phrase is captured both audibly and visually. Since anticipating this phrase is highly unlikely, general verification that the requested phrase was indeed spoken indicates a person willing to be captured on camera is attempting authentication. This verification can be accomplished with an ordinary audio speech recognizer. This device provides a confidence level that the phrase spoken was actually the phrase requested.

A visual test may be implemented to make sure that the sound articulated by the lips of the user matches the prompted phrase recognized in the received audio signal. The process of matching speech visually was described in Figure 10. This process can be aided by synchronization of the audio and visual transcripts as shown in Figure 19 where each frame of video is matched with a segment of the received audio transcript.

Referring now to Figure 20, voice authentication is provided. At some previous time, each authenticated user's voiceprint was characterized and stored. Each random phrase subsequently generated for authentication is compared to the appropriate known voiceprint. This process can be implemented such that at least a portion of the received audio signal is compared against the known words and phrases for verification. Alternatively, it is possible to use entirely random phrases provided the user's voiceprint can be modeled and/or the manner in which the user articulates phonemes can be determined from information previously obtained.

A visual recognition test may also be used. For example, a video segment of the recorded random phrase may be compared against how the user is known to articulate certain sounds. Various features may be extracted for this comparison such as, for example, lip shape.

Referring now to Figure 21, user authentication is provided, provided that the accessor performs satisfactorily during the described tests or tasks. Based on the results of each previous check, a decision is made as to whether or not the user attempting authentication is who he or she purports to be. If the decision is close, additional verification steps may be requested or additional tests may be performed on data already acquired.

Referring now to Figure 22, optional assessments may be provided by further analysis audio visual transcript. These include examining audio and visual data to determine the user's mental alertness, emotional state, sincerity, and the like.

Techniques for such assessment are available in the current art.

Such information may be used, for example, to determine if the user is intoxicated and should not be permitted to drive or open a weapons closet.

Finally Figure 23 summarizes this sample audio visual dynamic user authentication process in flowchart form.

Claims

What is claimed is:

1. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a means of recording a transcript of the attempted access,
    b. A communication link for transmitting the transcript and
    c. A means of receiving the transcript on the remote secure system or database.

2. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with a microphone for recording the transcript of the attempted access.

3. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with a camera for recording the transcript of the attempted access.

4. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with a fingerprint sensor for recording the transcript of the attempted access.

5. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with a signature capture device for recording the transcript of the attempted access.

6. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with a retinal scanner for recording the transcript of the attempted access.

7. A system for authenticating a user for a user as in claim (1) where in the access device is equipped with an iris scanner for recording the transcript of the attempted access.

8. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a means of recording a transcript of the attempted access,
    b. A communication link for transmitting the transcript,
    c. A means of receiving the transcript on the remote secure system or database,
    d. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task,
    e. A method for verifying the correctness of the task performed by the accessor,
    f. A method for verifying the biometric associated with the task and

g. A method for deciding whether or not to allow access to the remote system or database.

9. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task comprising
    a. Generating a random phrase of an unanticipated word or string of words and
    b. Prompting the accessor to say the said random phrase.

10. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task as in claim (9) where in a microphone captures the utterance of the phrase.

11. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task as in claim (9) where in a camera captures at least the mouth region of the accessor uttering the phrase.

12. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task comprising
    a. Generating a random finger movement across a fingerprint sensor and
    b. Prompting the accessor to perform the said movement.

13. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task comprising
    a. Generating a random phrase of an unanticipated word or string of words and
    b. Prompting the accessor to write or script the said random phrase.

14. A method for presenting the accessor with an element of surprise task request which prompts the accessor to perform unanticipated task comprising
    a. Generating a random set of cursor movements for the accessor to follow with his or her eyes and
    b. Prompting the accessor to follow the cursor as it moves in the said fashion.

15. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a microphone for recording an audio transcript of the attempted access,
    b. A communication link for transmitting the transcript,
    c. A means of receiving the transcript on the remote secure system or database,
    d. A method for presenting the accessor with a random phrase unanticipated by the accessor,
    e. A method for verifying the correctness of the spoken phrase captured by the audio transcript,
    f. A method for analyzing the audio transcript to verify that the voice print of the accessor captured by the transcript matches the voice print of the authorized user the accessor claims to be and

g. A method for deciding whether or not to allow access to the remote system or database.

16. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a camera for recording a video transcript of the attempted access,
    b. A communication link for transmitting the transcript,
    c. A means of receiving the transcript on the remote secure system or database,
    d. A method for presenting the accessor with a random phrase unanticipated by the accessor,
    e. A method for analyzing the video transcript to verify that the lip movements of the accessor captured by the transcript match the lip movements anticipated during the utterance of the prompted phrase,
    f. A method of analyzing the video transcript to verify that the face captured by the transcript matches the face of the authorized user the accessor claims to be and
    g. A method for deciding whether or not to allow access to the remote system or database.

17. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a microphone and a camera for recording an audiovisual transcript of the attempted access,
    b. A communication link for transmitting the transcript,
    c. A means of receiving the transcript on the remote secure system or database,
    d. A method for presenting the accessor with a random phrase unanticipated by the accessor,
    e. A method for analyzing the video transcript to verify that the lip movements of the accessor captured by the transcript match the lip movements anticipated during the utterance of the prompted phrase,
    f. A method for verifying the correctness of the spoken phrase captured by the audio transcript, and
    g. A method for deciding whether or not to allow access to the remote system or database.

18. A system for authenticating a user as in claim (17) also comprising a method of analyzing the video transcript to verify that the face captured by the transcript matches the face of the authorized user the accessor claims to be.

19. A system for authenticating a user as in claim (17) also comprising a method for analyzing the audio transcript to verify that the voice print of the accessor captured by the transcript matches the voice print of the authorized user the accessor claims to be.

20. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a fingerprint sensor for recording the fingerprint of the accessor,
    b. A communication link for transmitting the fingerprint sensor data,
    c. A means of receiving the data on the remote secure system or database,
    d. A method for presenting the accessor with a random finger movement unanticipated by the accessor to be replicated on the fingerprint sensor,
    e. A method for analyzing the fingerprint data to verify that the finger movements of the accessor captured by the data match the finger movements prompted,
    f. A method of analyzing the fingerprint data to verify that the fingerprint captured matches the fingerprint of the authorized user the accessor claims to be and
    g. A method for deciding whether or not to allow access to the remote system or database.

21. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a pressure sensor for recording writing or drawings made by the accessor,
    b. A communication link for transmitting the pressure sensor data,
    c. A means of receiving the pressure sensor data on the remote secure system or database,
    d. A method for presenting the accessor with a random phrase unanticipated by the accessor to be written on the pressure sensor,
    e. A method for verifying the correctness of the written phrase captured by the pressure sensor,
    f. A method for analyzing the pressure sensor data to verify that the writing style of the accessor captured by the sensor matches the writing style of the authorized user the accessor claims to be and
    g. A method for deciding whether or not to allow access to the remote system or database.

22. A system for authenticating a user for access to a remote secure system or database comprising
    a. Access device equipped with a camera for recording a video transcript of the attempted access,
    b. A communication link for transmitting the transcript,
    c. A means of receiving the transcript on the remote secure system or database,
    d. A method for presenting the accessor with a random cursor movement unanticipated by the accessor, which the accessor has to follow with his or her eyes
    e. A method for analyzing the video transcript to verify that the eye movements of the accessor captured by the transcript match the eye movements anticipated during the movement of the cursor,

f. A method of analyzing the video transcript to verify that the eyes captured by the transcript match the eyes of the authorized user the accessor claims to be and
g. A method for deciding whether or not to allow access to the remote system or database.

23. A system for authentication a user for access to a remote secure system or database as in claim (22) wherein the method for verifying that the eye is captured by the transcript match the eyes of the authorized user the accessor claims to be includes the retinal scan of at least one of the accessor's eyes.

24. A system for authentication a user for access to a remote secure system or database as in claim (22) wherein the method for verifying that the eye is captured by the transcript match the eyes of the authorized user the accessor claims to be includes the iris scan of at least one of the accessor's eyes.

25. A method for analyzing the video transcript to verify that the lip movements of the accessor captured by the transcript match the lip movements anticipated during the utterance of the prompted phrase comprising
    a. A generic model for the lip movements associated with the prompted phrase,
    b. Analysis of the video transcript to extract the features of lips,
    c. A method for comparing the generic model with the features of the lips to produce a likelihood of correspondence.

26. A method for analyzing the video transcript as in claim (25) wherein the method also includes a means for deciding whether the likelihood of the correspondence merits deeming that the model and the transcript match.

27. A method for analyzing the video transcript as in claim (25) wherein the model is customized for the accessor.

28. A method for analyzing the video transcript as in claim (25) wherein the model is more specific given selected attributes of the accessor.

FIGURES

Figure 1.

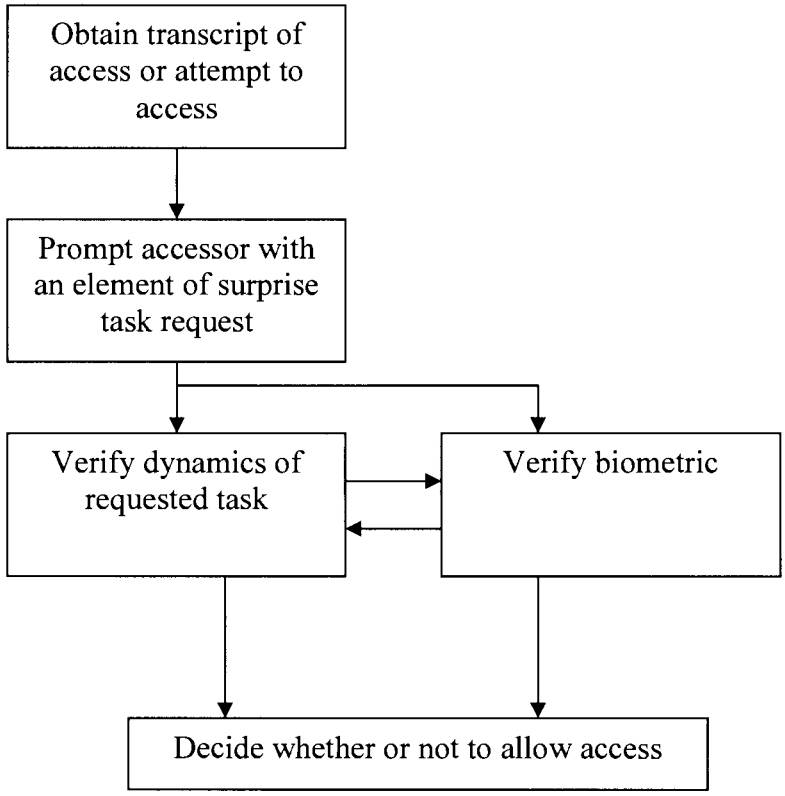


Figure 2.

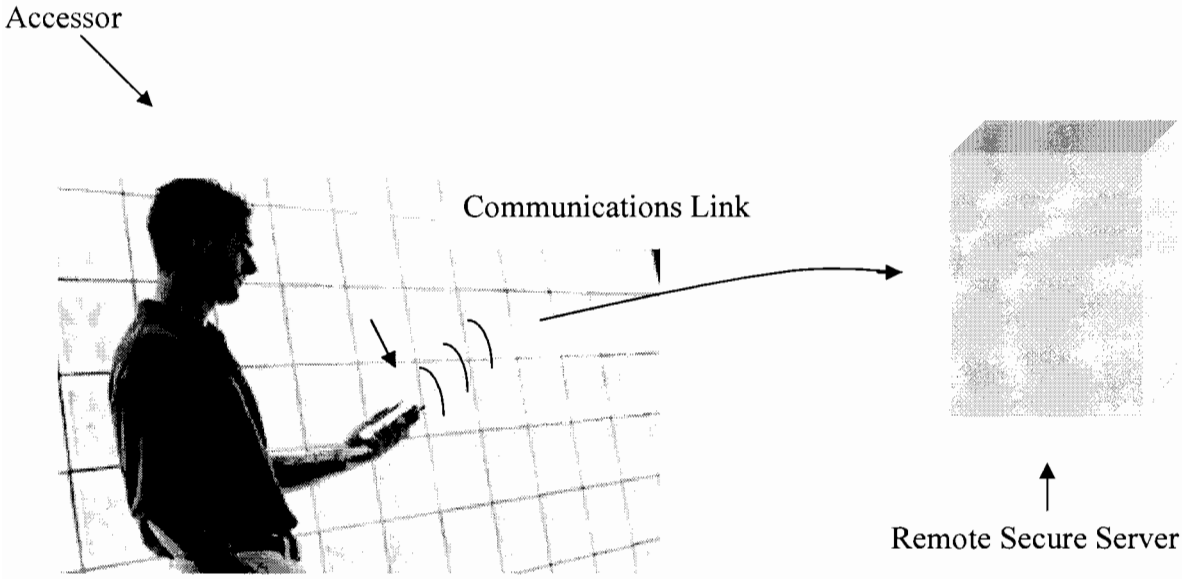


Figure 3.

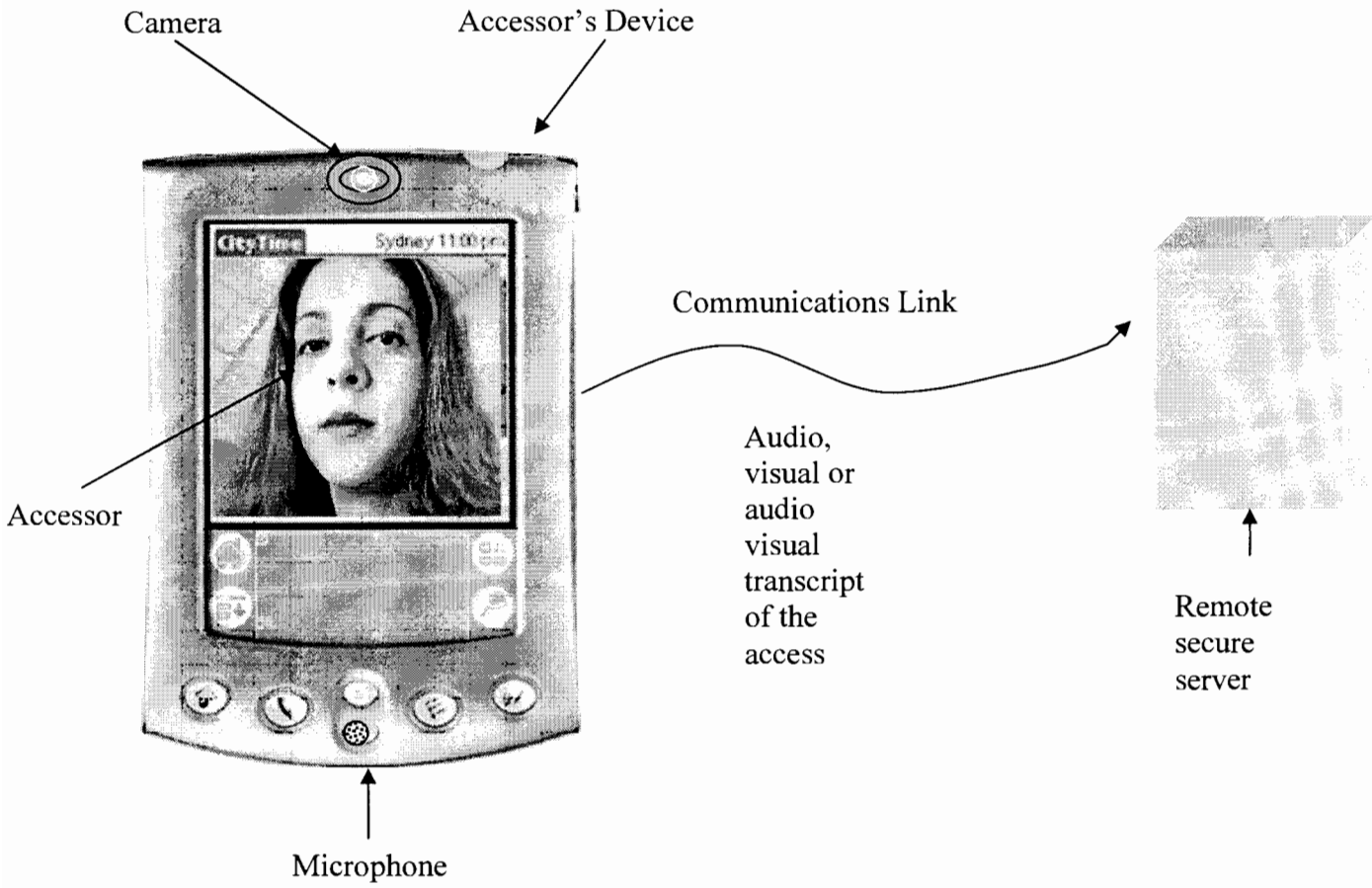

Camera
Accessor's Device
Communications Link
Audio, visual or audio visual transcript of the access
Accessor
Remote secure server
Microphone

Figure 4.

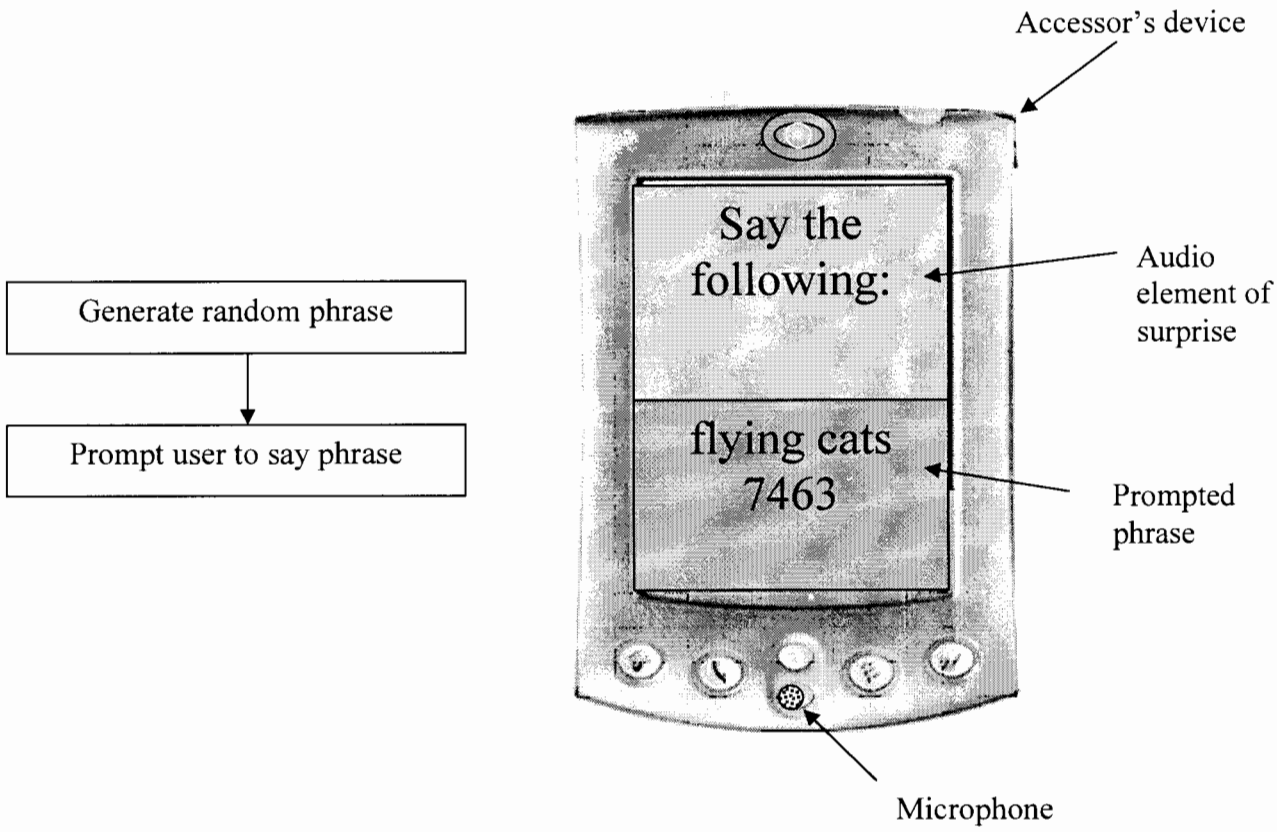

Generate random phrase
Prompt user to say phrase
Accessor's device
Say the following:
flying cats 7463
Audio element of surprise
Prompted phrase
Microphone

Figure 5.

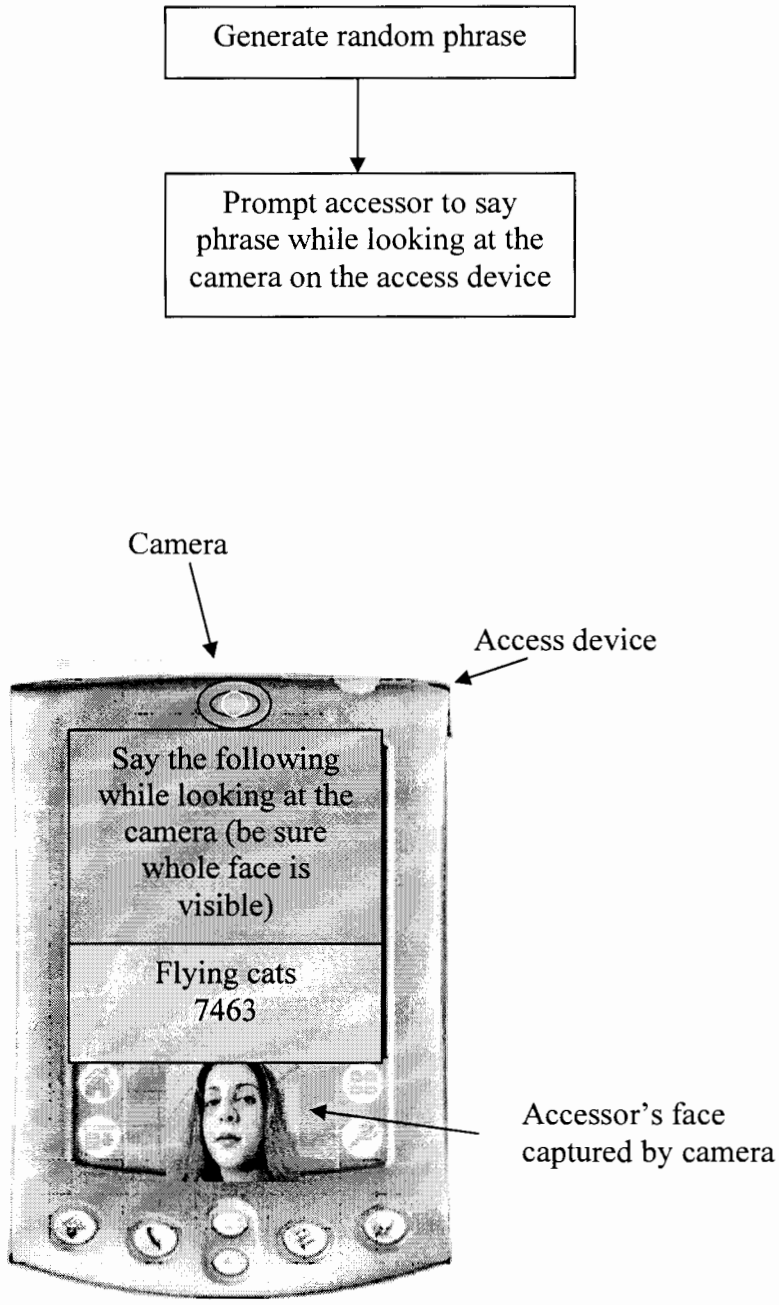

Generate random phrase
Prompt accessor to say phrase while looking at the camera on the access device
Camera
Access device
Say the following while looking at the camera (be sure whole face is visible)
Flying cats
7463
Accessor's face captured by camera

Figure 6. An element of surprise using the fingerprint sensor

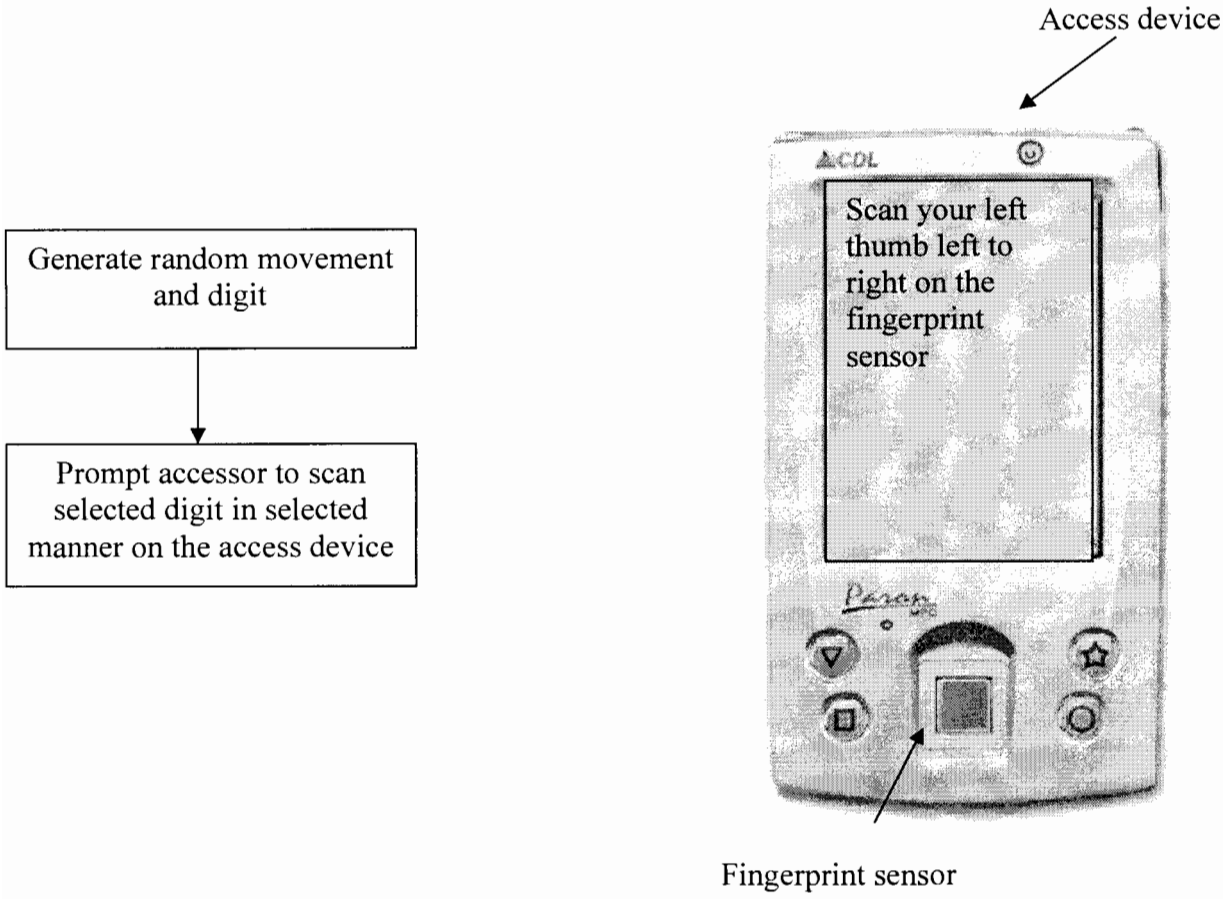


Figure 7.

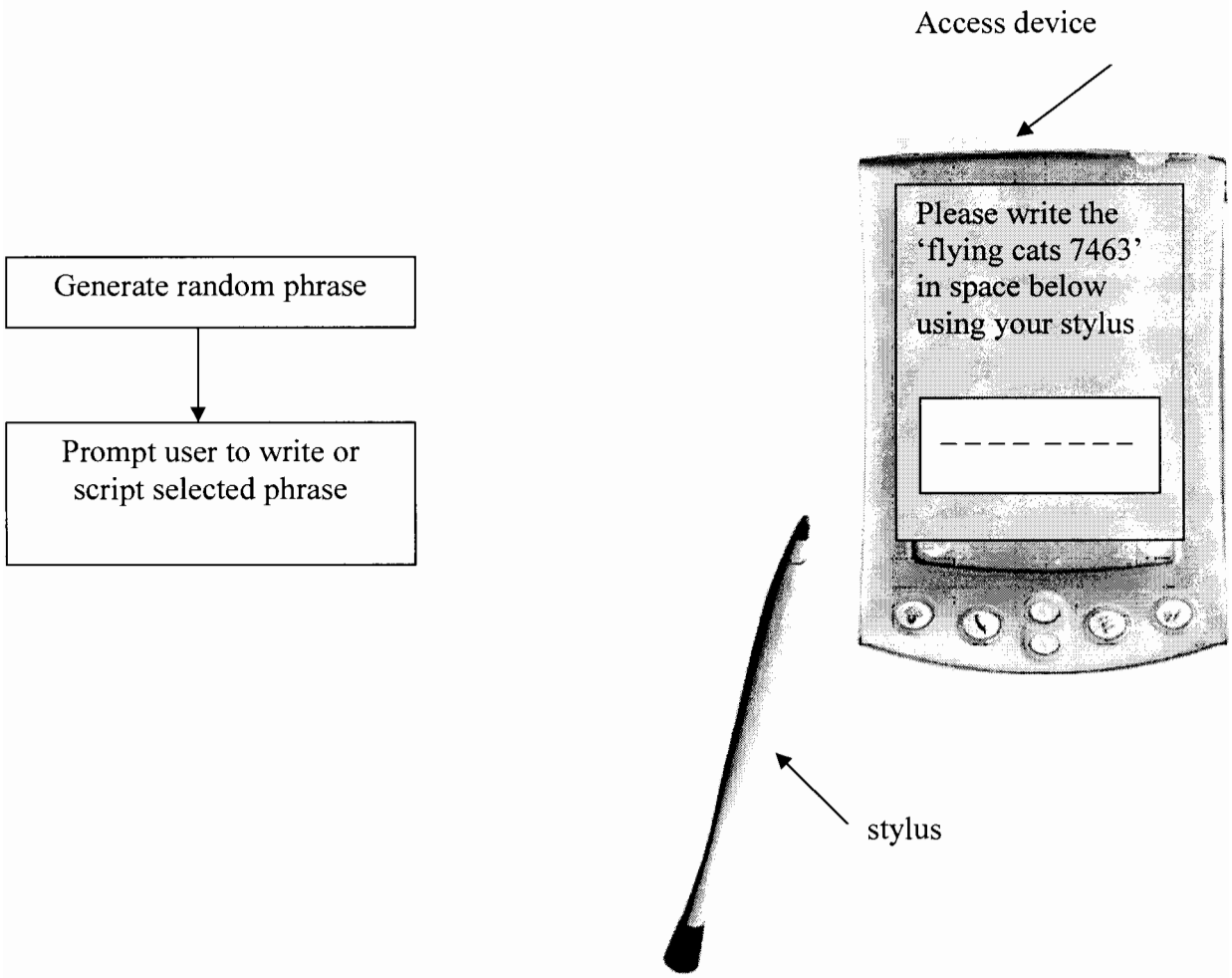
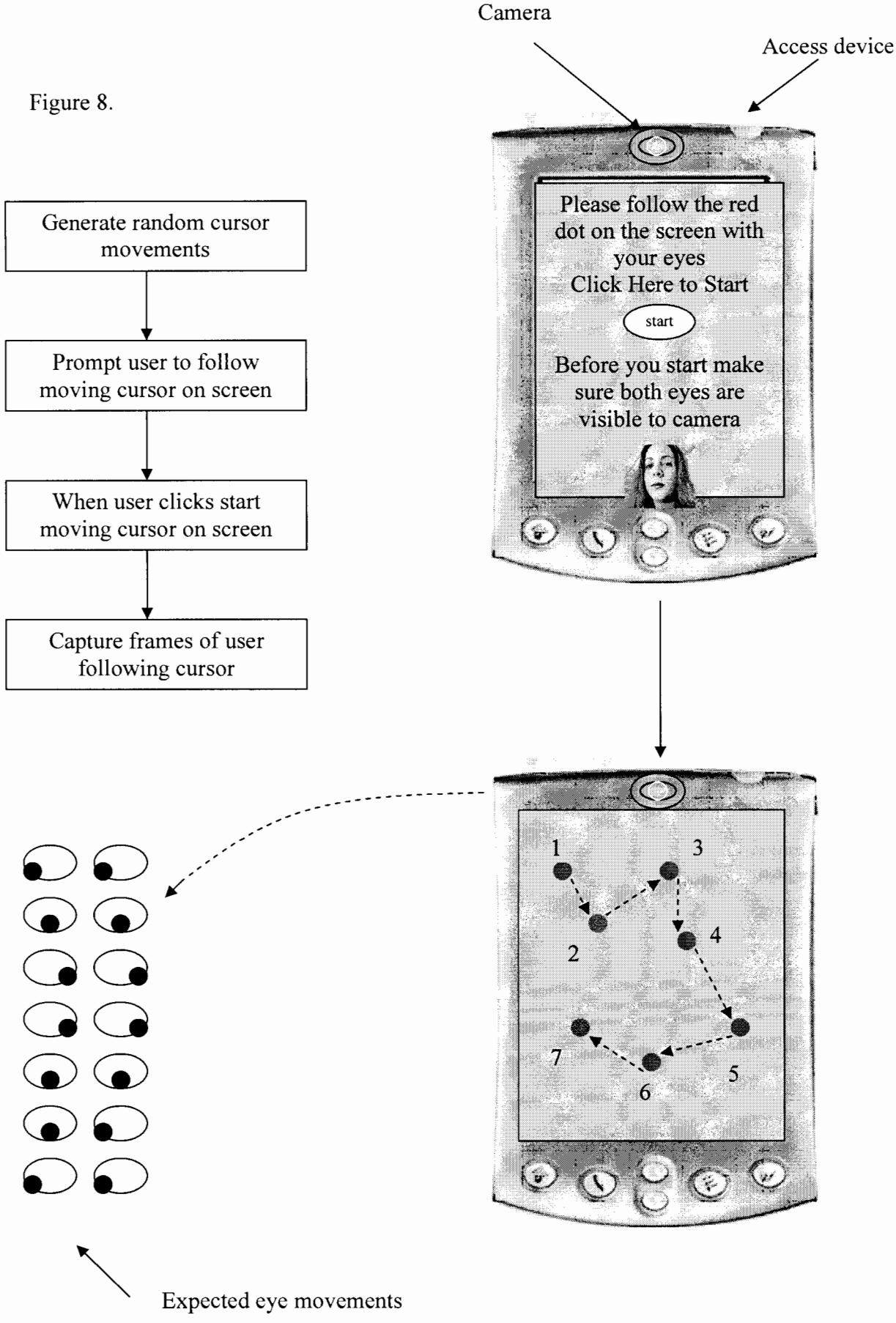

Generate random phrase
Prompt user to write or script selected phrase
Access device
Please write the 'flying cats 7463' in space below using your stylus
stylus

Figure 8.


Camera
Access device
Generate random cursor movements
Prompt user to follow moving cursor on screen
When user clicks start moving cursor on screen
Capture frames of user following cursor
Please follow the red dot on the screen with your eyes
Click Here to Start
start
Before you start make sure both eyes are visible to camera
1
2
3
4
5
6
7
Expected eye movements

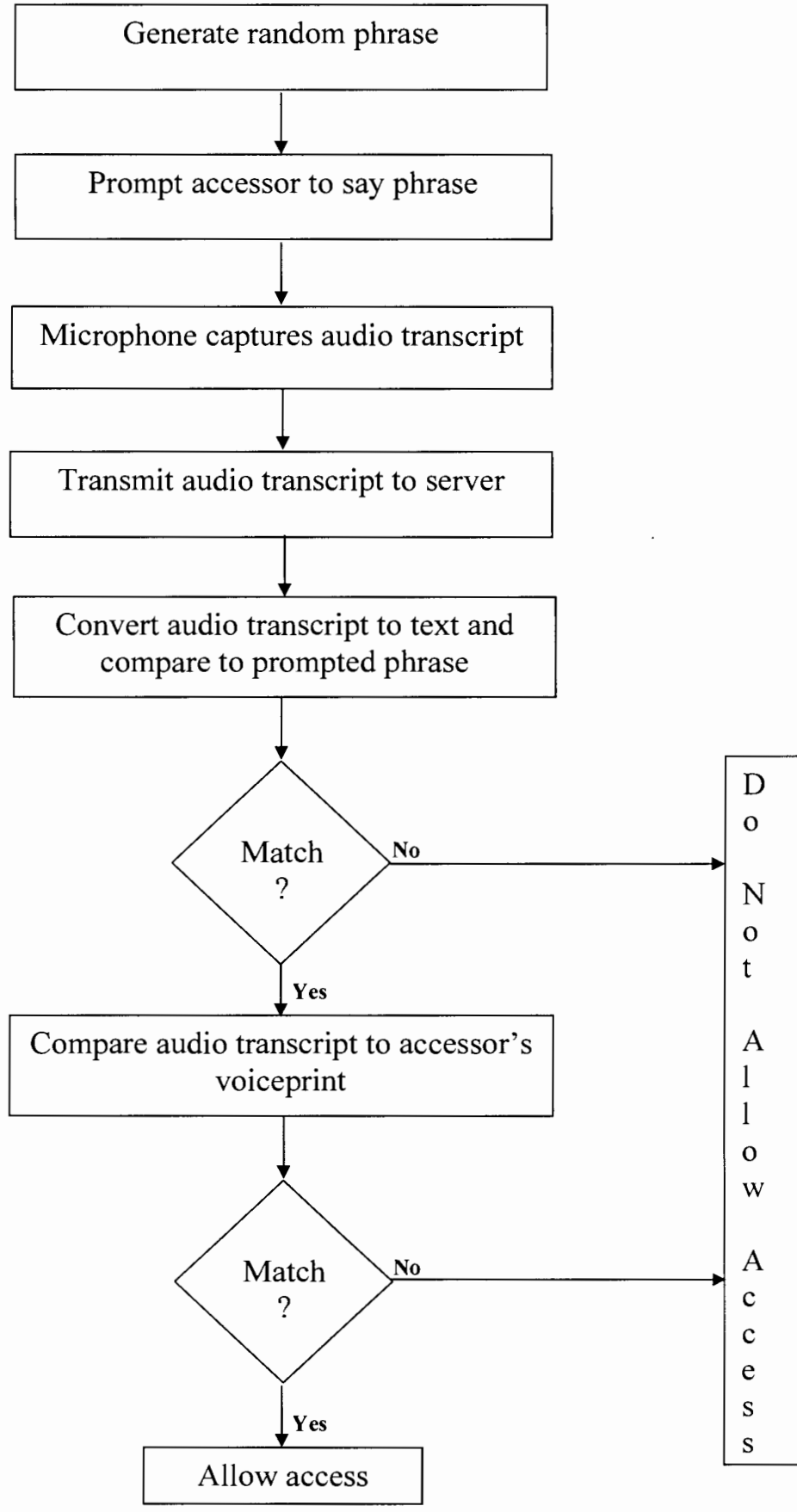

Generate random phrase
Prompt accessor to say phrase
Microphone captures audio transcript
Transmit audio transcript to server
Convert audio transcript to text and compare to prompted phrase
Match ?
No
Yes
Compare audio transcript to accessor's voiceprint
Match ?
No
Yes
Allow access
Do Not Allow Access

Figure 9.

Figure 9.

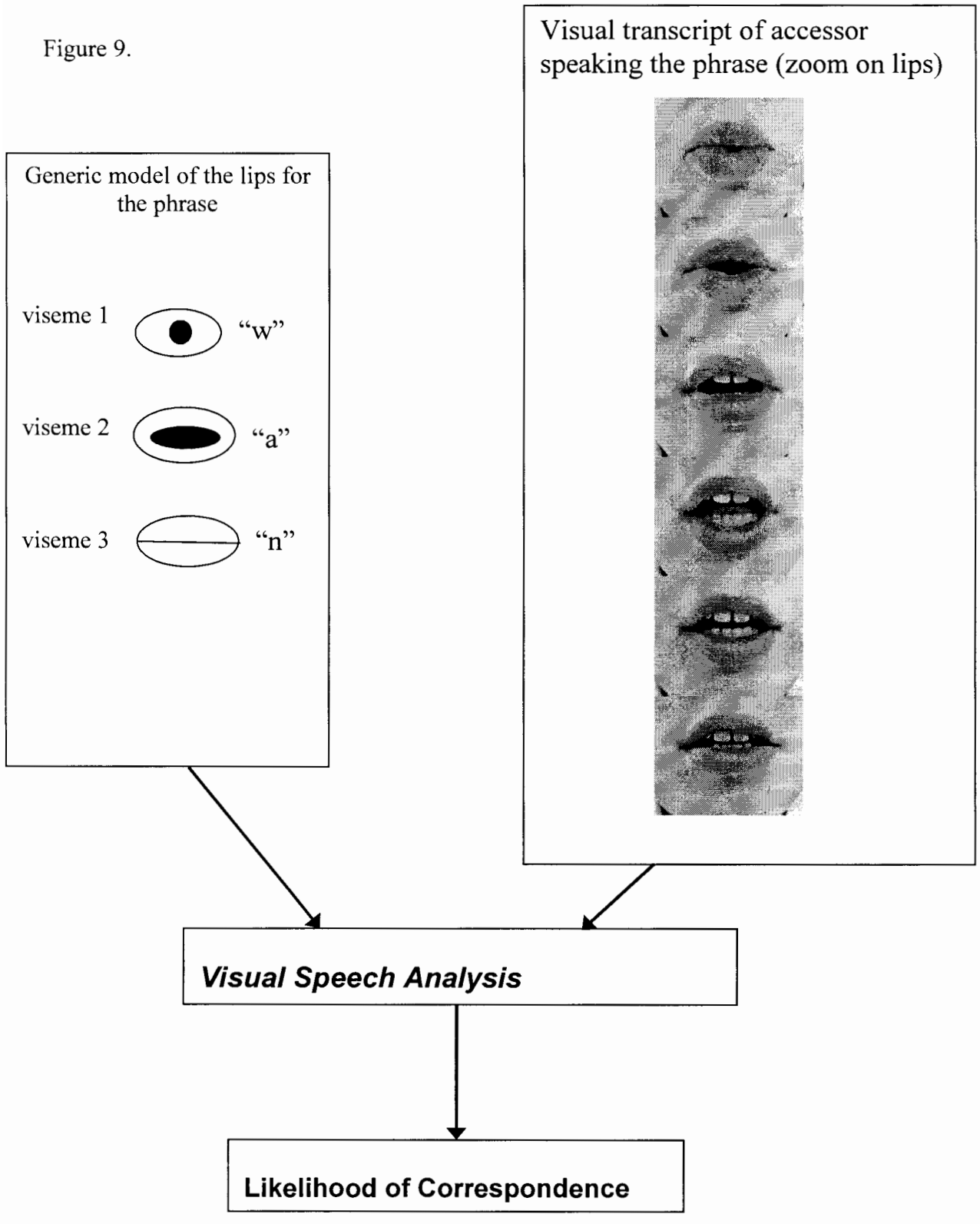

Visual transcript of accessor speaking the phrase (zoom on lips)
Generic model of the lips for the phrase
viseme 1
"w"
viseme 2
"a"
viseme 3
"n"
Visual Speech Analysis
Likelihood of Correspondence

Figure 10.

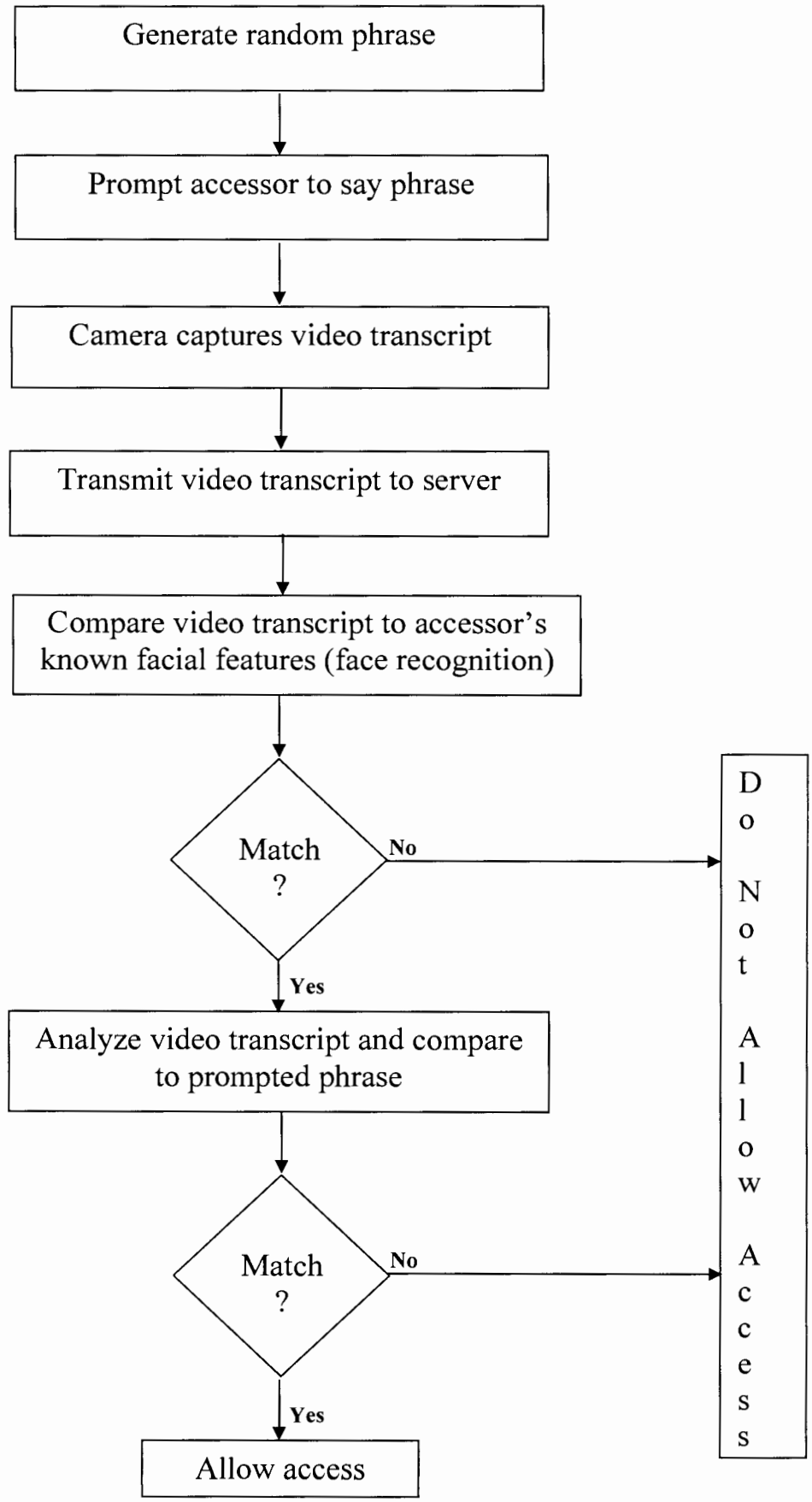

Generate random phrase
Prompt accessor to say phrase
Camera captures video transcript
Transmit video transcript to server
Compare video transcript to accessor's known facial features (face recognition)
Match ?
No
Yes
Analyze video transcript and compare to prompted phrase
Match ?
No
Yes
Allow access
Do Not Allow Access

Figure 11.

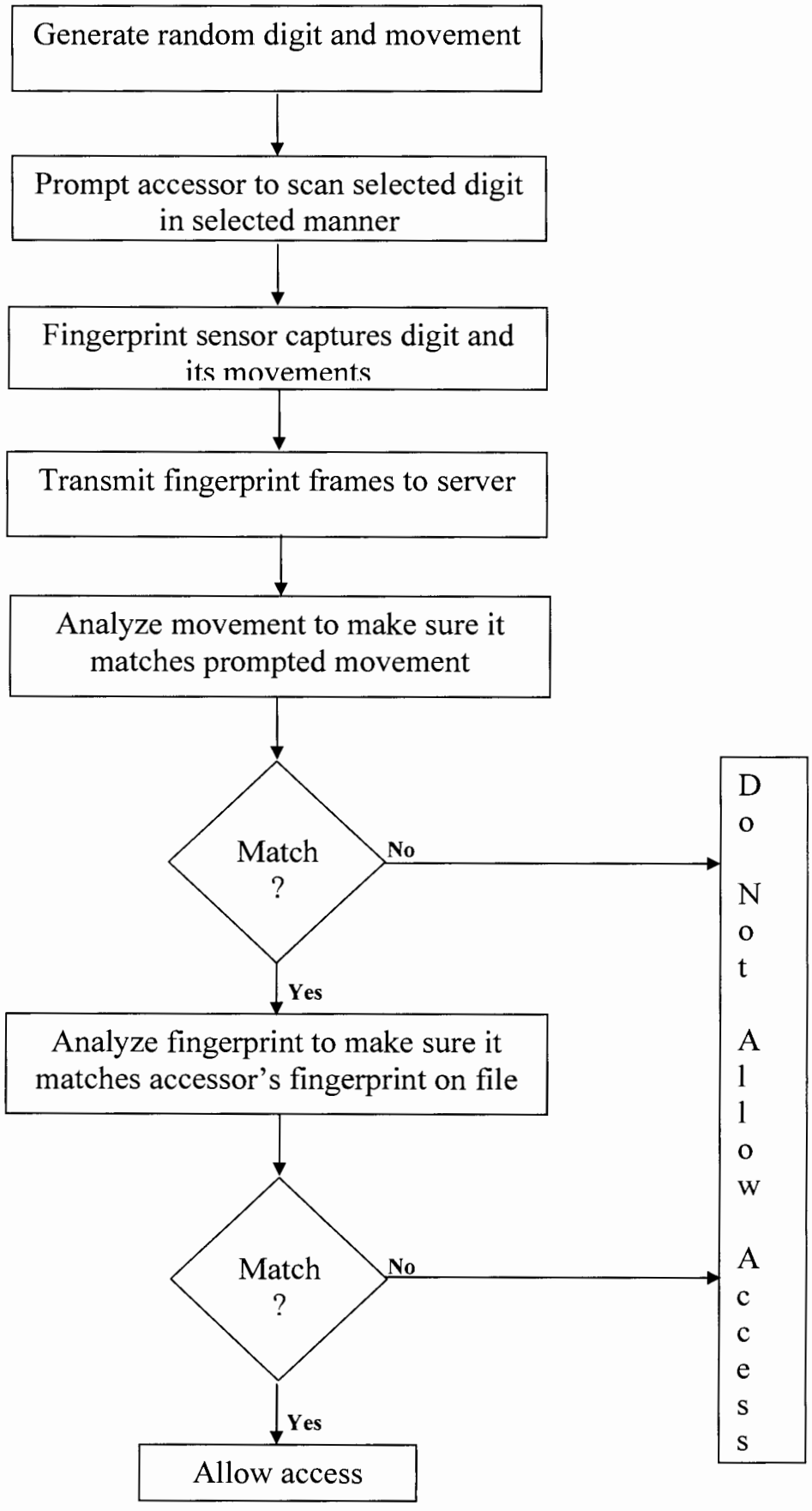

Generate random digit and movement
Prompt accessor to scan selected digit in selected manner
Fingerprint sensor captures digit and its movements
Transmit fingerprint frames to server
Analyze movement to make sure it matches prompted movement
Match ?
No
Yes
Analyze fingerprint to make sure it matches accessor's fingerprint on file
Match ?
No
Yes
Allow access
Do Not Allow Access

Figure 12.

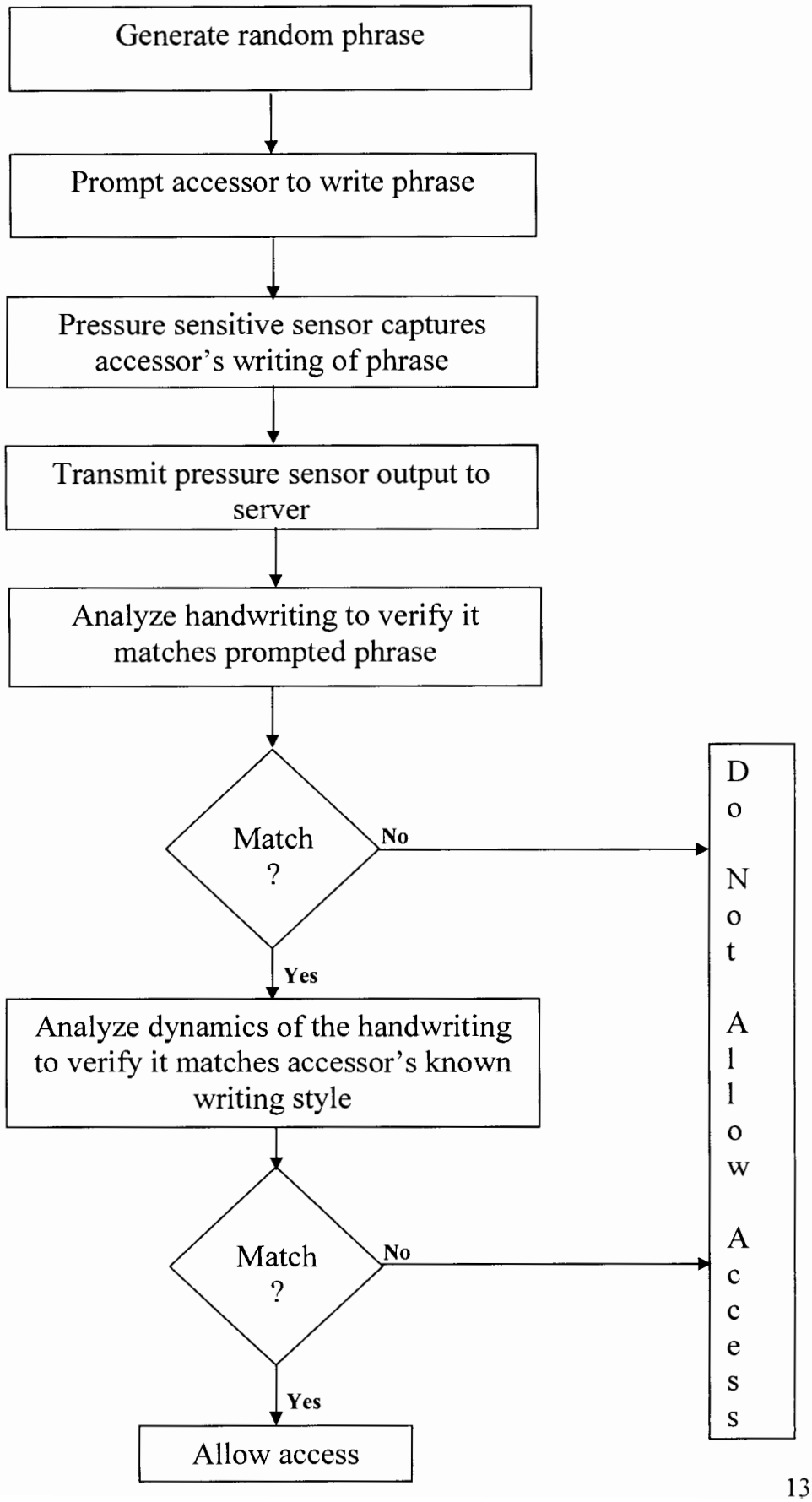

Generate random phrase
Prompt accessor to write phrase
Pressure sensitive sensor captures accessor's writing of phrase
Transmit pressure sensor output to server
Analyze handwriting to verify it matches prompted phrase
Match ?
No
Yes
Analyze dynamics of the handwriting to verify it matches accessor's known writing style
Match ?
No
Yes
Allow access
Do Not Allow Access

Figure 13.

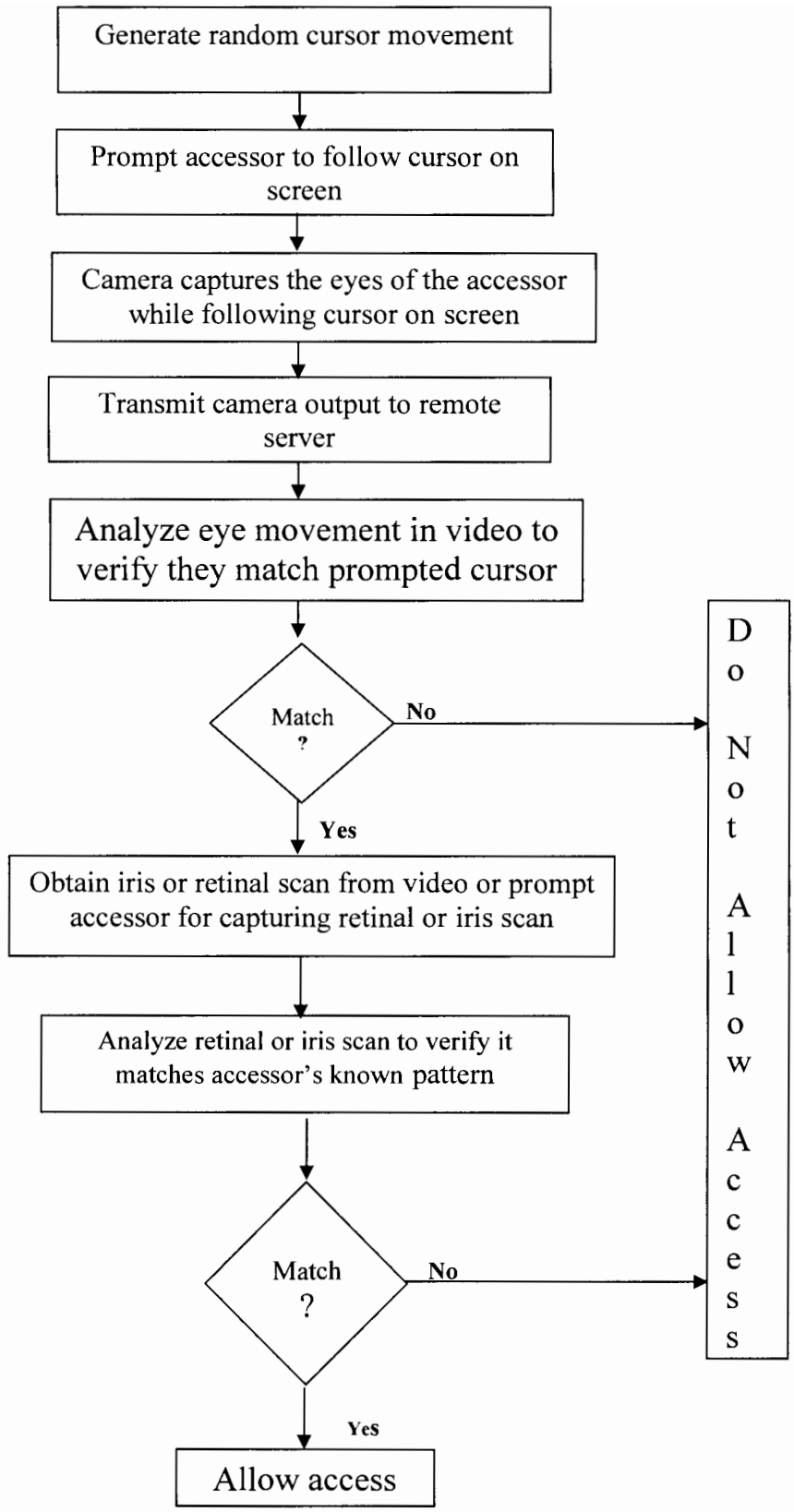

Generate random cursor movement
Prompt accessor to follow cursor on screen
Camera captures the eyes of the accessor while following cursor on screen
Transmit camera output to remote server
Analyze eye movement in video to verify they match prompted cursor
Match ?
No
Yes
Do Not Allow Access
Obtain iris or retinal scan from video or prompt accessor for capturing retinal or iris scan
Analyze retinal or iris scan to verify it matches accessor's known pattern
Match ?
No
Yes
Allow access

Figure 14. Iris recognition

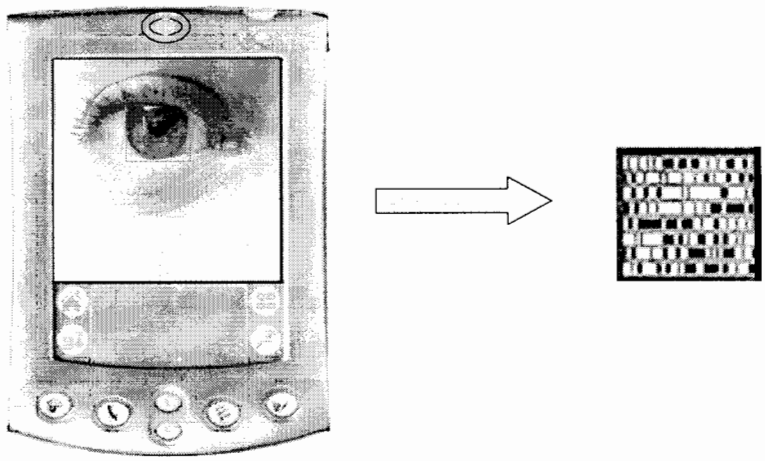


Figure 15.

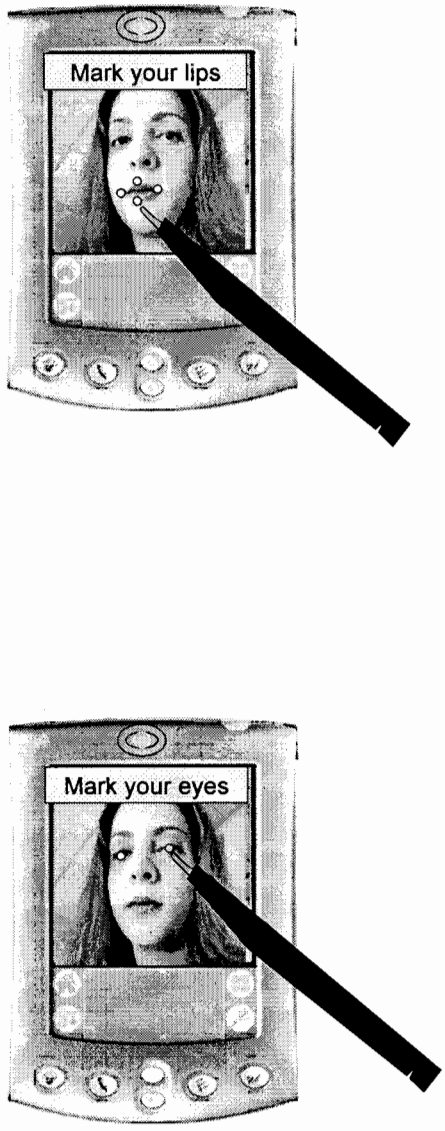


Figure 16.

Figure 17.

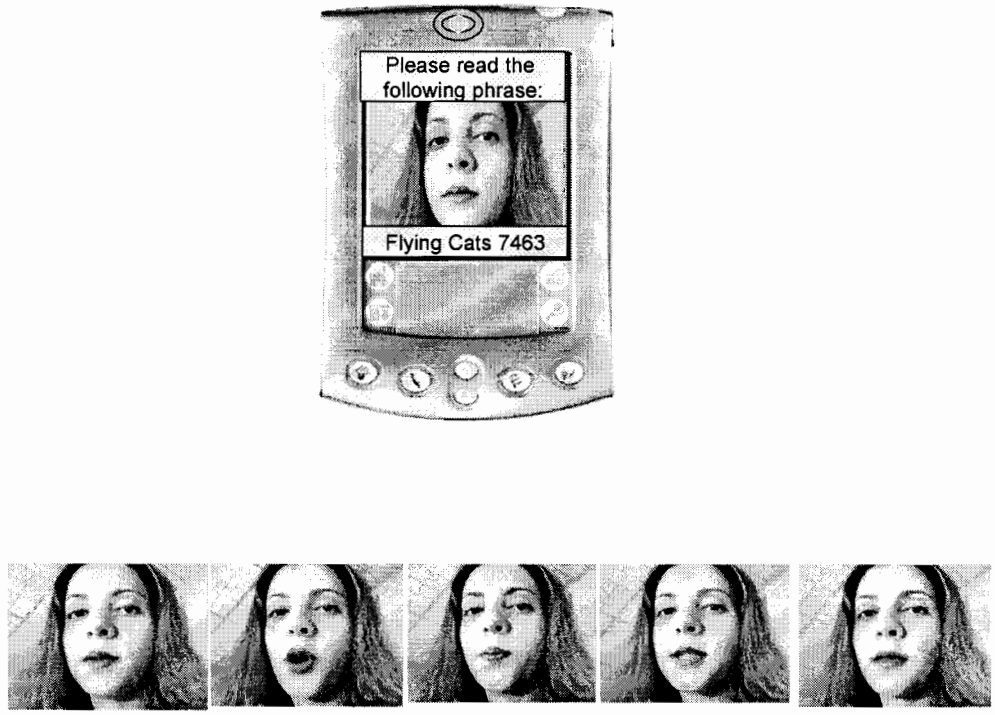


Figure 18.

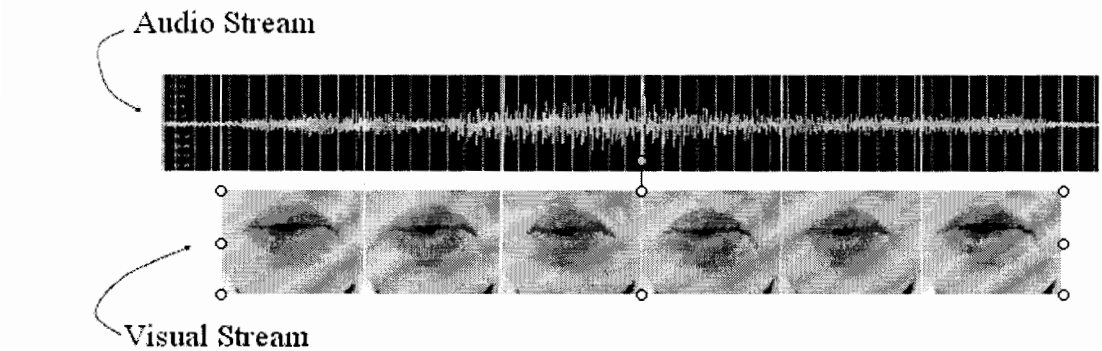


Figure 19.

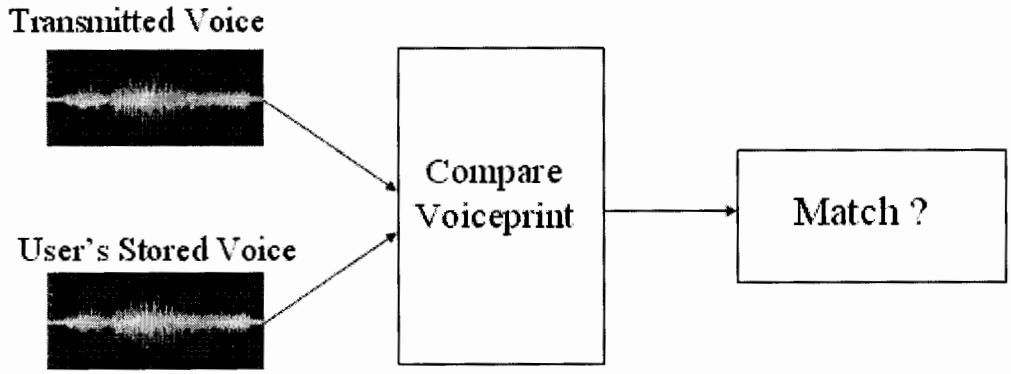

Transmitted Voice
User's Stored Voice
Compare Voiceprint
Match ?

Figure 20.

Figure 21.

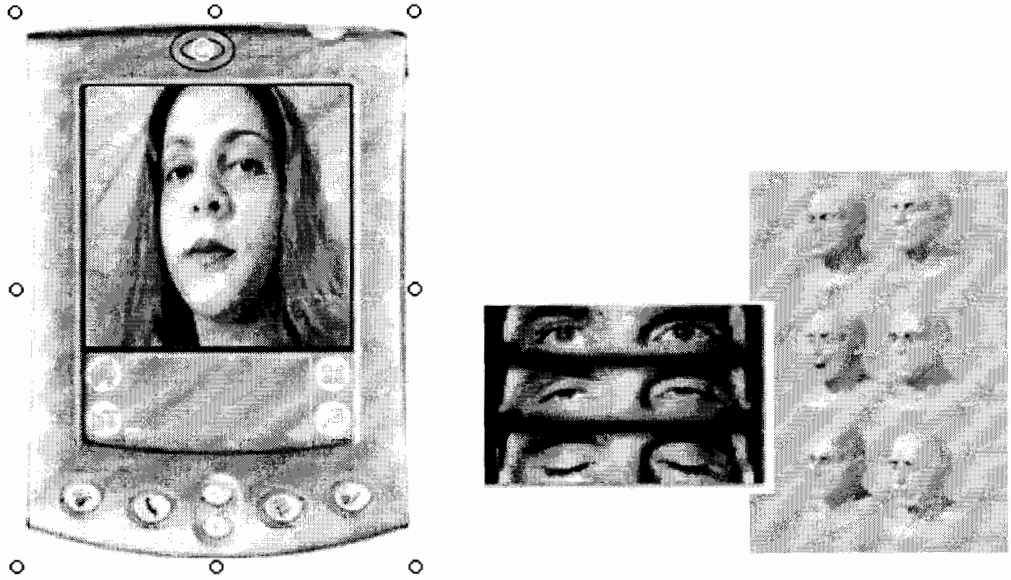
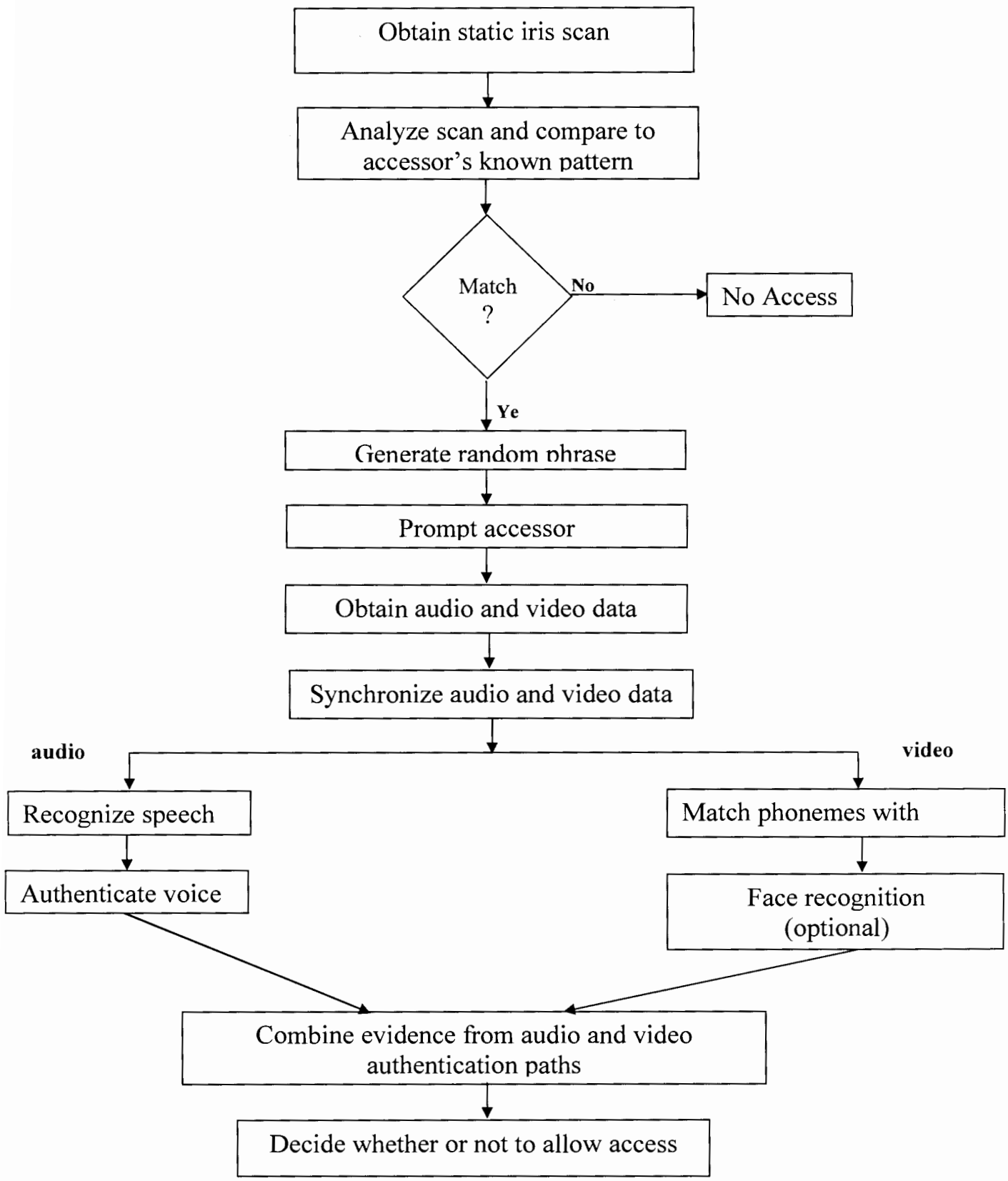


Figure 22.


Obtain static iris scan
Analyze scan and compare to accessor's known pattern
Match ?
No
No Access
Ye
Generate random phrase
Prompt accessor
Obtain audio and video data
Synchronize audio and video data
audio
video
Recognize speech
Authenticate voice
Match phonemes with
Face recognition (optional)
Combine evidence from audio and video authentication paths
Decide whether or not to allow access