Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2904646 A1 2016/03/15

(21) 2 904 646

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2015/09/15

(41) Mise à la disp. pub./Open to Public Insp.: 2016/03/15

(30) Priorité/Priority: 2014/09/15 (IN2646/DEL/2014)

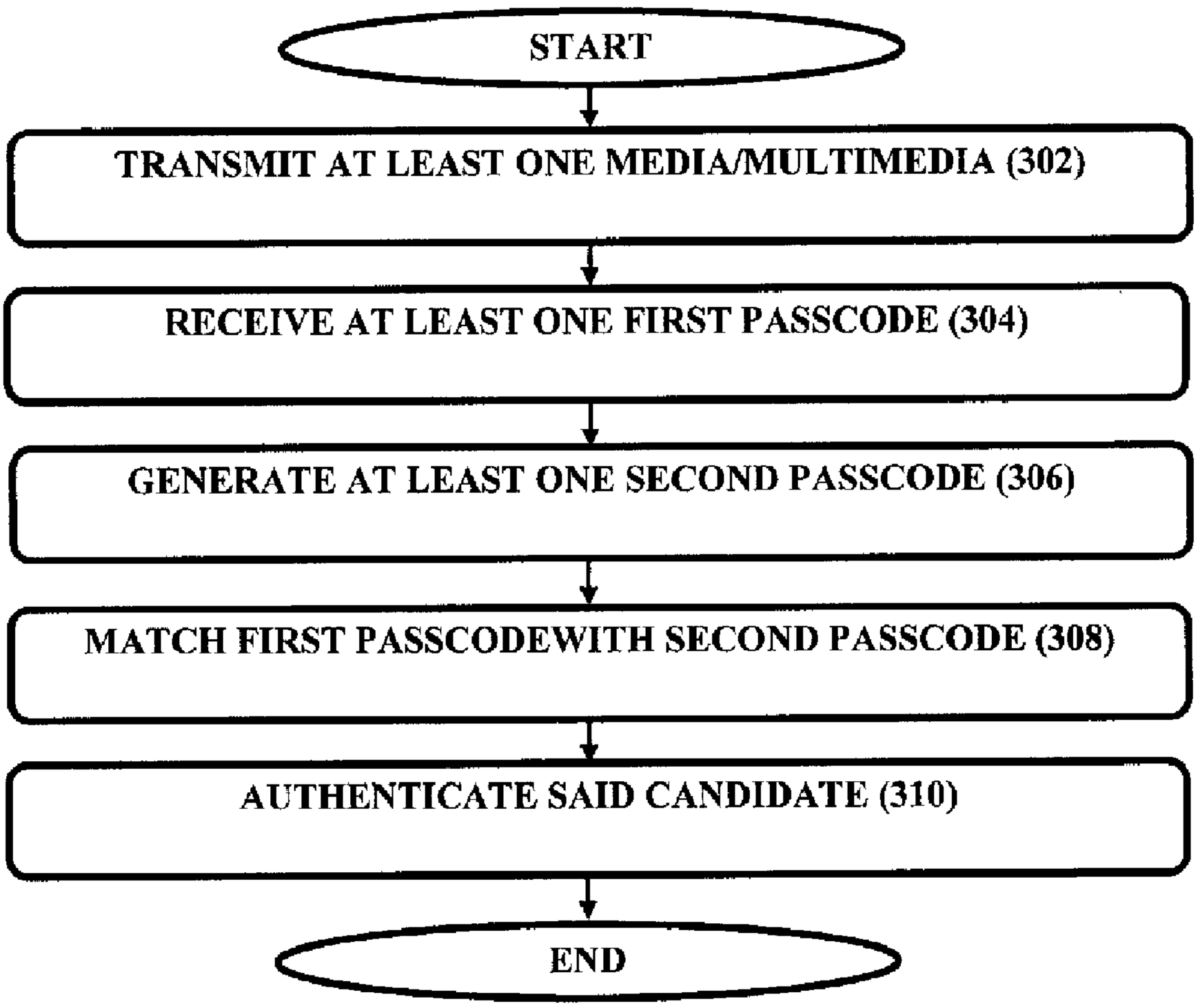
(51) Cl.Int./Int.Cl. *G06F 21/30* (2013.01)

(71) Demandeurs/Applicants:
THE REGISTRAR, GRAPHIC ERA UNIVERSITY, IN;
GOYAL, PUNEET, IN

(72) Inventeurs/Inventors:
GOYAL, PUNEET, IN;
KHANNA, NITIN, IN;
SHYAM, RADHEY, IN;
CHAUHAN, JOOHI, IN

(74) Agent: RICHES, MCKENZIE & HERBERT LLP

(54) **Titre : AUTHENTIFICATION SECURISEE EMPLOYANT UN CODE DE SAUT**
(54) **Title: SECURE AUTHENTICATION USING DYNAMIC PASSCODE**



(57) **Abrégé/Abstract:**
Methods and systems for secure authentication using dynamic passcode are disclosed. In one implementation, candidate specifies the mapping that the candidate plans to use for generating the dynamic passcode by either visiting the branch office and/or some

CA 2904646 A1 2016/03/15

(21) 2 904 646

(13) A1

(57) **Abrégé(suite)/Abstract(continued):**
secure communication media. During the authentication phase, as per the present invention, the candidate receives at least one media/multimedia from the authenticating server. The candidate replies with a dynamic passcode generated using candidate-specific mapping and elements related to media/multimedia transmitted to the candidate. Accordingly, authentication is based upon the media/multimedia transmitted, candidate- specific mapping pre-stored and the dynamic passcode received.

ABSTRACT

SECURE AUTHENTICATION USING DYNAMIC PASSCODE

Methods and systems for secure authentication using dynamic passcode are disclosed. In one implementation, candidate specifies the mapping that the candidate plans to use for generating the dynamic passcode by either visiting the branch office and/or some secure communication media. During the authentication phase, as per the present invention, the candidate receives at least one media/multimedia from the authenticating server. The candidate replies with a dynamic passcode generated using candidate-specific mapping and elements related to media/multimedia transmitted to the candidate. Accordingly, authentication is based upon the media/multimedia transmitted, candidate-specific mapping pre-stored and the dynamic passcode received.

(TO BE PUBLISHED WITH FIGURE 3)

SECURE AUTHENTICATION USING DYNAMIC PASSCODE

CROSS-REFERENCE OF THE RELATED APPLICATION

This application claims priority to Indian Patent Application No. 2646/DEL/2014, filed with the Indian Patent Office on September 15, 2014 and entitled "**SECURE AUTHENTICATION USING DYNAMIC PASSCODE**", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The present subject matter described herein, in general, relates to information/data security and/or authentication, and more particularly to a usable secure authentication.

BACKGROUND

Secure Authentication is a crucial aspect for any organization or nation, especially now when world is so much online connected. Although still applicable, but before the beginning of this massively online era, legitimate users used to be authenticated primarily on the basis of their physical presence and/or some valid ID/information. For example: Access to some defense lab is provided only after the security guard visually identifies the person and verifies his/her ID card; The banks or other financial organizations earlier used to allow user to withdraw money from his/her account only after verifying his/her identity and the passbook issued to him/her by the bank. Withdrawal of money using cheque is then later introduced and is allowed only after someone presents to the bank, the valid cheque that was issued to the customer by the bank and after customer's signature's verification. Today in the globally connected world and with almost everyone accessing internet resources (net-banking, e-commerce, ATM, e-governance, e-payments, online reservations, e-mail, e-learning, online exams, remote medical consultation, tele-conference, remote video surveillance, mobile banking, cloud services, etc.), both usability and security have become demanding goals for any authentication system to be widely accepted. Other considerations associated with authentication methods and systems are – cost effectiveness, feasibility, compatibility to existing infrastructure, etc.

Conventional authentication systems generally rely on factors such as - Something you know (such as PIN, password), something you have (ATM/debit/credit card, hardware token device like RSA SecurID, OTP receiving/generating device like mobile phone), and

Something you are (such as biometrics - fingerprints, retinal scan, face recognition etc.). Behavioural characteristics (such as typing pattern) of the user have also been considered as one of the factors for authentication but these are rarely used and currently not so reliable. Biometric based authentication systems are often costly and not easily deployable for it requires new hardware and software installations. Also, biometrics is not changeable so even stolen once anywhere will lead to insecurity forever for all the users whose biometrics data is stolen. Single factor authentication schemes are mostly password based because it is cost effective and simple, but passwords present implicit contradiction between usability (short, easy to remember) and security (difficult to guess/crack). Also, with the users generally having multiple accounts (leading to use of same password for easy remembrance, writing/storing multiple passwords) and attackers having high performance computing systems to try to crack easily, password based schemes are not generally appreciated. To prevent against automated guessing/DDOS attacks, many times CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) images are generally used, but passwords etc. still do get compromised because of attacks like phishing, Trojan/malware based, key-logging, shoulder-surfing, spying etc.Also, the single factor authentication systems (such as passface/passpoints based systems), and in general, currently used single band authentication systems are implicitly not considered much secure because of snooping, man-in-the-middle (MITM) and other security attacks, which makes it easier for the attackers to succeed sooner or later.

Two-factor authentication (TFA) schemes address many of these security concerns, for these generally require either use of additional hardware device (like RSA SecurID, ATM/Credit card reader) or personal mobile devices (for receiving/generating one time passcode i.e. OTP), in addition to the user password, at the time of authentication. The prior-art document US 6993658 discloses a password setting system for a secure system includes a user token server and a communication module, wherein the user concatenates the secret passcode with the random token received (on personal communication device, such as a mobile phone or a pager carried by the user) in order to form a valid password, which is then used for authentication.

Another prior-art document US 8566916 B1 ('916) discloses a method, system, and apparatus for agile generation of one time pass codes (OTPs). The '916 makes use of selecting a variance technique from a set of variance techniques and generating the OTP

according to this selected variance technique. At the validator, not only OTP is compared but also the variance technique used by the token generator to generate the OTP.

Another prior-art document US 20080168543 A1 ('543) discloses a method/system including a number generator residing on a first server to generate first and second OTP tokens from a shared clock, a transmitter residing on the first server to transmit the first and the second OTP tokens, a receiver residing on a second server to receive the first, the second, and a third OTP tokens, and a comparator residing on the second server to compare the second and the third OTP tokens to authenticate an identity of a party who generates the third OTP token.

Another prior-art document US 20130185780 A1 ('780) discloses a system to generate a OTP without using a hardware token, but uses the client machine where some functions and parameters are generated and transmitted to, by the server. In '780, the client generates a first OTP using a predefined function on the token and the hash value of user password, such that retrieving the hash value of the password from the first OTP is a discrete log problem. Further, in '780 a second OTP is generated using a bilinear mapping on the first OTP, such that generating first OTP from second OTP is a bilinear inverse problem.

The additional hardware device requirement in TFA schemes not only adds to the cost (generally in distribution, replacement, maintenance, disposal etc.) but also to user inconvenience, as user needs to carry an additional device, and device can also get stolen. These problems become more severe if one were to carry multiple additional devices for multiple accounts.

Furthermore, the available TFA based systems, where personal mobile devices may be used for receiving OTP via., SMS and then same OTP is then sent (generally Out-of-Band OOB) to authenticate, have been susceptible to sim-cloning, sim-swap, cellular-network attacks, device-theft, Trojan and other attacks, and there have been reported several successful security frauds in recent years in relation to these. In some scenarios like ATM withdrawals, SMS OTP based authentication systems are difficult to use for the delays often associated with receiving OTP via SMS. Some solutions relying on using personal devices (like Smartphone, iPADs, personal computer) for executing the application that generates OTP in sync with authentication server (using common seed) or decrypts the encrypted OTP received, have also been proposed but these are again susceptible to device-theft and malware/Trojan attacks. Also, these solutions are limited to those who possess smartphones/PCs which may not be the case especially in many developing countries.

Also, with the large number of phishing and similar attacks occurring every year, knowing/acquiring user credentials have become much easier and thus such device-dependent TFA schemes have become more like those which are authenticating the devices and not the user who really needs to be authenticated. Security issues further get complicated because of general lack of awareness about good security practices and some undesirable habits/practices of the users like not regularly changing the authentication key, sharing password with family members/friends at times (sometimes carelessly, sometimes because of need like bad health, travelling but no internet access, etc.).

It is therefore dire need to develop more secure and usable authentication systems and methods.

SUMMARY

This summary is provided to introduce concepts related to a system and method therefor secure authentication using dynamic passcode generated with candidate specific mapping and the concepts are further described below in the detailed description. The summary is illustrative only and is neither intended to identify essential features of the claimed subject matter nor is it intended for use in determining or limiting the scope of the claimed subject matter.

The present invention addresses one of more of the above-described problems of the existing authentication systems and a technical solution is achieved in the present invention by providing security measures such that, the system is much more secure and also reasonably usable. The authentication system as per the present invention is secure even if OTP SMS is compromised that may be via sim-cloning, sim-swap, etc., or one's personal device (that receives/generates OTP) is compromised (that may be via Trojan, malware, stolen, etc.); or one's password is compromised that may be via key-logging attack, shoulder-surfing attack, password once shared with some friend/colleague, etc.

In one implementation, the present invention discloses a technique using which candidate shares initially one or more mapping(s) specific to oneself that would be used for generating the transformed passcode (transformed media/multimedia) by either visiting the branch office and/or some secure communication media. In one implementation, the candidate specific mapping(s) are distributed to the specific candidate via registered post or via some other secure means.

In one implementation, the present invention discloses a technique in which during the authentication phase, candidate is conveyed the media/multimedia content (like an OTP text, OTP embedded within some other multimedia like audio/image/video/animation etc.,) from the authenticator (authenticating system or server or its representative) on candidate's device (like phone, personal computer, iPad, or some other device used during authentication). The candidate replies with the first passcode which is a transformed media/multimedia (in either text or multimedia form) that is generated using candidate-specific mapping and the media/multimedia content conveyed initially. This candidate-specific mapping is generally neither stored on any user device nor it is transmitted over the communication channel. The media/multimedia conveyed to the candidate is valid for authentication purpose only for specific limited opportunities like for limited number of authentication sessions and/or for limited time period only (for e.g. 15 mins, 1 hour, 1 day, etc.).

In one implementation, the media/multimedia content comprises two or more elements, the elements are preferably selected from alpha numeric values, ASCII characters, roman characters, regional language characters, symbols or some other form of information. For example, media/multimedia content is text "47683245" where its eight elements are 4, 7, 6, 8, 3, 2, 4 and 5. Two or more of these elements would be used for generating the dynamic passcode using the candidate specific mapping. In one implementation, the elements of the media/multimedia transmitted are randomly generated (e.g. OTP).

In one implementation, the present invention discloses a technique to generate a transformed media/multimedia using the candidate-specific mapping (without necessarily using any software or hardware on the candidate side). So, the present method is secure even against those attacks or security breaches where the client/candidate side system/device or the information shared during authentication over the communication device or channel is once compromised or stolen or intercepted.

In one implementation, the candidate-specific mapping used for generating the first passcode includes at least one parameter selected from a group of parameters involving data associated with a current or past transaction/authentication session (like credit/debit account number, amount of money, etc.), unvarying data known to both said candidate and said authenticator (like candidateID, candidate's date of birth, etc.), varying data accessible to both said candidate and said authenticator (like day, month, year, time, date, region related information when/where access is requested, etc.), or any combination thereof.

In one implementation, the candidate specific mapping used for generating the first passcode includes the mathematical operations, logical operations, permutations, conditionals, or some other operations/mappings including customized operations/mappings. These operations are preferably applied on elements associated with the initially transmitted media/multimedia content and elements associated with the other parameters/data associated with the candidate-specific mapping, in order to generate the valid passcode as authentication key for that particular authentication session. The wide range of mappings available to choose from, enhances the security significantly and making it difficult to guess for the attackers to succeed.

In one implementation, the present invention discloses a technique to deal with how the media/multimedia transmitted is transformed using candidate-specific mapping and/or some parameters, and then the transformed media/multimedia is used for authentication.

The authenticator also independently generates the second passcode using the media/multimedia content (one that was initially transmitted) and the candidate-specific mapping (and its associated parameters value) associated with that candidate. This second passcode is compared with the first passcode received from the candidate and accordingly the authentication is performed.

In one implementation, an authenticator for authenticating a candidate is disclosed. The authenticator comprises a transmitter module, in responsive to detecting an access request, configured to transmit at least one media/multimedia; a receiver module configured to receive at least one first passcode from said candidate, wherein said first passcode is a transformed media/multimedia obtained from said media/multimedia transmitted; a passcode matching module configured to generate at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate, and match said transformed media/multimedia with said second passcode generated; an authentication module, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate.

In one implementation, a method for authenticating a candidate by an authenticator is disclosed. The method comprises:

- transmitting, in responsive to detecting an access request, at least one media/multimedia;

- receiving at least one first passcode, wherein said first passcode is a transformed media/multimedia, wherein said transformed media/multimedia obtained from said media/multimedia transmitted;
- generating at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate;
- matching said transformed media/multimedia with said second passcode generated; and
- authenticating, in responsive to the match of said transformed media/multimedia with said second passcode, said candidate.

In one implementation, a system for authenticating a candidate is disclosed. The system comprises an authenticator including a transmitter module, in responsive to detecting an access request, configured to transmit at least one media/multimedia; a receiver module configured to receive at least one first passcode from said candidate, wherein said first passcode is a transformed media/ multimedia obtained from said media/ multimedia transmitted; a passcode matching module configured to generate at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate, and match said transformed media/multimedia with said second passcode generated; an authentication module, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate; and at least one device communicably coupled to said authenticator and configured to provide or enable selection of said candidate-specific mapping for storing in said candidate database, wherein said candidate-specific mapping are pre-stored and customizable.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

The exemplification set out herein illustrates preferred embodiments of the invention, in one form, and such exemplification is not to be construed as limiting the scope of the invention in any manner.

Figure **1** illustrates a network implementation of a system, in accordance with an embodiment of the present subject matter.

Figure **2** illustrates an authenticator for authenticating a candidate, in accordance with an embodiment of the present subject matter.

Figure **3** illustrates a method for authenticating a candidate, in accordance with an embodiment of the present subject matter.

Figure **4** illustrates a method for storing candidate-specific mapping (and associated parameters)in the candidate database, in accordance with an embodiment of the present subject matter.

It is to be understood that the attached drawings are for purposes of illustrating the concepts of the invention and may not be to scale.

DETAILED DESCRIPTION OF THE EMBODIMENTS

In order to make the aforementioned objectives, technical solutions and advantages of the present application more comprehensible, embodiments are described below with accompanying figures.

The objects, advantages and other novel features of the present invention will be apparent to those skilled in the art from the following detailed description when read in conjunction with the accompanying drawings.

While the invention is described along with several embodiments and illustrative drawings, it should be understood that the invention is not limited to any one embodiment, but instead includes numerous equivalents. For example, while most of the embodiments are described in the context of simple text as media/multimedia content, those skilled in the art will recognize that the disclosed systems and methods are readily adaptable for other media/multimedia contents as well. For example, without limitation, the present invention could be readily applied in the context of image, audio, video, animations or interactive content forms as media/multimedia content. In addition, for providing a thorough understanding of the present approach, numerous specific details are set forth in the following description; the present approach may be practiced by not including all or some of these details. Moreover, for the purpose of clarity, certain technical material that is known in the art related to the invention has not been described in detail in order to avoid unnecessarily obscuring the present invention.

The word candidate used throughout the present invention refers to one making access request, preferably selected from a human user, an artificial intelligence (AI) system, a robot and the like. The person skilled in the art may understand that the usage of the word/expression "candidate" shall not restrict the protection scope of the present invention.

In one implementation, the present invention disclose various mechanisms/ techniques to ensure and enhance the security for user authentication even when OTP SMS/information is once compromised or one's personal device (that receives/generates OTP) is once compromised or one's password is once somehow compromised or information shared over communication device or channel is compromised.

In one implementation, the candidate may share initially with the authenticating server (bank system, etc.) one or more specific mapping(s) that one plans to use for generating the dynamic passcode (which is used finally for authentication), by either visiting the branch office and/or some secure communication media. In one implementation, candidate specific mapping(s) may also be distributed to the specific candidate via registered post or via some other secure means.

In one implementation, during the authentication phase, the candidate is conveyed the media/multimedia content from the authenticating server. In one implementation, the media/multimedia conveyed to the candidate is valid for authentication purpose only for specific limited opportunities like for limited number of authentication sessions (generally for one-time only) and/or for limited time period only (for e.g. 15 mins, 1 hour, 1 day, etc.). The candidate replies with the dynamic passcode which is a transformed media/multimedia that is generated using original media/multimedia content and the candidate-specific mapping (and its associated parameters).

In one implementation, the media/multimedia conveyed to the candidate is based on randomly generated code (like OTP). In one implementation, the way for candidate to access the media/multimedia could be any from a group comprising of email or SMS/MMS or communicated via web-browser or application running on candidate's device (in sync with the authentication server) or via some electronic device (like ATM, token device like SecurID, Access control mechanisms devices at doors, etc.), and combinations thereof.

In one implementation, the media/multimedia content comprises two or more elements, the elements are preferably selected from alpha numeric values, ASCII characters, roman characters, regional language characters, symbols or some other form of information. For example, media/multimedia content is text "47683245" where its eight elements are 4, 7, 6, 8, 3, 2, 4 and 5. Herein this example the elements are numeric values but it is also well understood by a person skilled in the art that the elements may not be limited to only numeric values but may include other ASCII characters or regional language characters or symbols also. Two or more of these elements may be used for generating the dynamic passcode using

the candidate specific mapping. It is also well understood that the media/multimedia content may also be an image or video or some other multimedia content with these elements embedded within.

In one implementation, the elements of the media/multimedia transmitted may be completely randomly selected/generated (e.g. OTP). In one implementation, the elements of the media/multimedia transmitted are generated randomly but with some constraints like the elements should all be distinct or only at most two duplicates of an element are allowed or the elements must belong from specific set of characters/symbols only, etc. The dynamic passcode used for authentication and generated using the candidate-specific mapping is based on these elements conveyed as/within media/multimedia transmitted by the authentication server to the candidate. The advantage of providing these elements in multimedia is to enhance the security against the automated guessing attacks even in cases when both the communication messages (the multimedia transmitted by the server and the dynamic passcode provided by the candidate) are intercepted without the knowledge of the candidate. This interception is generally extremely difficult if communication channels used are different (like in out of band authentication systems) but may be possible if using single-band authentication. For single-band authentication, it may be preferred to provide multiple multimedia (like several CAPTCHA images) for candidate to choose from, so that security is further enhanced.

In one implementation, the said candidate-specific mapping may not be stored or transmitted over the communication channel.

In one implementation, for the authentication or secure transaction, the candidate who initiates the transaction or authentication request, the candidate who receives (or gets access to) the media/multimedia content transmitted and the candidate who replies with the transformed/dynamic passcode for authentication to proceed further – they may not be all the same. For example, in some corporate banking solution, a user initiates the transaction or authentication request. Another or same user receives (or gets access to) the media/multimedia content transmitted by the authenticating server, and provides to his/her colleague or superior or the user who initiated the transaction. That user now generates the dynamic passcode (or say, transformed media/multimedia) using this and his/her specific mapping (and associated parameters), which is then responded back to the server by the same person or different user, which is then compared with the expected passcode, and only if it matches, the transaction or authentication request is approved. In one implementation, the

system receiving the access request, the system transmitting the media/multimedia content to the candidate, and the system that receives the dynamic passcode from the candidate and matches with the second passcode computed separately at system level – these systems may not be all the same, although they may be communicating or sharing some common resources/information/database.

In one implementation, the limited access is provided depending on comparison/matching result (for e.g. match with different second passcodes may facilitate different degree of access, in some scenarios), In one implementation, the honey pot system may also get activated depending on comparison/matching result, especially in case of some suspicious behavior (for e.g. match with some specific second passcode from given plurality of second passcodes may facilitate initiating honey pot trap in some scenarios).

In one implementation, the candidate-specific mapping used for generating the first/second passcode includes at least one parameter selected from a group of parameters involving data associated with a current or past transaction/authentication session (like credit/debit account number, amount of money, etc.), unvarying data known to both said candidate and said authenticator (like candidateID, candidate's date of birth, etc.), varying data accessible to both said candidate and said authenticator (like day, month, year, time, date, region related information when/where access is requested, etc.), or any combination thereof. In one implementation, the elements associated with the above mentioned parameters may be mapped to numeric values or some other characters or symbols, before applying the candidate specific mapping to compute the dynamic passcode. For example, the first three letters corresponding to the day when authentication is attempted (or it may also be the previous day or the next day or day of the same date but previous month) may be mapped as per the order in which the alphabets appear in the English language (A – 01, B-02,…M-13, N-14, O-15, …. Z-26); so Monday is mapped to 131514. Some other candidate may have chosen the ASCII values corresponding to these days prefix.

In one implementation, the candidate-specific mapping used for generating the first/second passcode includes the mathematical operations, logical operations, permutations, conditionals, or some other operations or mappings including customized operations or mappings. These operations are preferably applied on elements associated with the initially transmitted media/multimedia content and elements associated with the other parameters/data associated with the candidate-specific mapping, in order to generate the valid passcode as

authentication key for that particular authentication session. In one implementation, the candidate specific mapping may be a series of mappings applied after one another.

In one implementation, the candidate-specific mapping is configured to generate at least one output, the output consists of two or more elements, and each element is wherein the output consists of two or more elements, and each element is independently based on at least one parameter selected from a group of parameters involving elements associated with said media/multimedia, data associated with a current or past transaction, unvarying data known to both said candidate and said authenticator like candidateID, varying data accessible to both said candidate and said authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

The elements of the output of the candidate specific mapping are independently computed, the candidate specific mapping is considered consisting of several mappings (or operations, likely but not necessarily mathematical operations) as per the number of elements in the output. The transformed media/multimedia thus generated using candidate-specific mapping may be simple concatenation or combination of these elements in the output or may be a multimedia where these elements are embedded within. In one implementation, the transformed media/multimedia (i.e. first passcode) may be a voice signal. Also, having the candidate-specific mapping as combination of element level mappings not only makes it easier for the people in general to apply these mappings (or computations)but also provides them the wide range of mappings (and associated parameters) to choose from; this not addresses the usability concerns but also enhances the security significantly and thus making it difficult to guess for the attackers to succeed.

Some of the examples of the candidate specific mappings (and associated parameters) used for generating the dynamic passcodes are provided below, however it is understood by the person skilled in the art that the below mentioned example are for mere understanding and the actual application of the present invention may have simpler or complex transformations:

Consider that media/multimedia received from the authenticating server is based on randomly generated code as "47683245" and its eight elements are 4, 7, 6, 8, 3, 2, 4 and 5, denoted using A, B, C, D, E, F, G and H respectively here. Also, the following examples presents mappings that comprises of 8 element-level mappings and thus generate output with 8 elements, but this is just for illustration purpose, it is well understood by those skilled in

the art that the size and combination of these elements in the output could be done in other ways also.

Candidate1chosen mapping

- ABCDEFGH → (A+B)(B+C)(C+D)(D+E)(E+F)(F+G)(G+H)(H+A)
    - All transformations over modulo 10 to have unit's digit place. We use ( ) to denote that the number considered would be the unit's digit of the number within ( )
  - 47683245→(4+7) (7+6)(6+8)(8+3)(3+2)(2+4)(4+5)(5+4)
    →(11)(13)(14)(11)(5)(6)(9)(9)
    →13415699 (Candidate 1 responds with this dynamic passcode).

Candidate 2 specific mapping (using unvarying data for e.g. 1, 2 and 3 here)

- ABCDEFGH →[H+1][A+2][(B*D+3)]G(C+D)(D+E)(E+F)(F+G)
  We use [ ] here to denote the mapping that maps y to (9-y).
- 47683245→33044156 (Candidate 2would be responding with this dynamic passcode).

Candidate 3 specific mapping (using varying data i.e. current date and a series of mappings)

- ABCDEFGH →Reverse of {ABCDEFGH + current date in ddmmyyyy format} (element level computations); and then applying operator [ ] on each alternate element. We use [ ] here to denote the mapping that maps y to (9-y).
    - let's say current date is 25 Mar 2013 (that means 25032013 in ddmmyyyy format)

  User calculates 47683245+25032013
  = (4+2)(7+5)(6+0)(8+3)(3+2)(2+0)(4+1)(5+3)
  =62615258
  Reverse is 85251626.
  Applying the next mapping i.e. operator [ ] on alternate element
  8[5]2[5]1[6]2[6] → 84241323
- 47683245→84241323 (Candidate 3would be responding with this dynamic passcode).

Candidate 4specific mapping (using conditionals)

ABCDEFGH →HGFEDCBA if H is odd, else ACEGABDF

- 47683245→54238674 (Candidate 4would be responding with this modified passcode)
- 47683254→46354782 (Candidate 4would be responding with this dynamic passcode as last digit of input is now even)

In one example, the other examples of candidate specific mappings may include but not limited to:

- ABCDEFGH → (A*B)(B*C)(C*D) …..(H*A)
- ABCDEFGH → (A*α)(B*β)(C*γ)(D*δ)(E*α)(F*β)(G*γ)(H*δ) where α, β, γ and/or δ could be some parameters dependent on transaction data (like last 4 digits of credit account number) or user PIN or varying data known to both user and authenticator (like time in hhmm format, or last 4 digits of PIN code of that region) or addition of these parameters.
- ABCDEFGH → (A*2)(B*2)(C*2) …..(H*2) if date is even, else (A*3)(B*3)(C*3) …..(H*3) if date is odd
- ABCDEFGH →$(A^{\alpha})(B^{\beta})(C^{\alpha})(D^{\beta})$…..$(G^{\alpha})(H^{\beta})$ --- α,β are some candidate specified parameters as discussed above
- ABCDEFGH → $(A^{B})(B^{C})(C^{D})$ …..(H^{A})
- ABCDEFGH → $(A^{A})(B^{B})(C^{C})$ …..(H^{H})

All mappings/transformations discussed above are over modulo 10 for each digit, but different candidate may choose other options as well. Some candidate-specific mappings may also use hard-core/customized mappings (like mapping 2 to 5 and vice-versa, mapping 9 to 6 and vice versa) in combination or independent of other mappings. Some candidate-specific mappings may also use alphanumeric or other characters as well like mapping A to 8, mapping 1 to!, etc. In some embodiments, some candidate specific mappings be such that it may map the media/multimedia transmitted like "ABCD" (having elements A, B, C, D) to the dynamic passcode "WXYZ". In some embodiments, this may be mapped to "123456" as per some candidate-specific mapping. In some embodiments, this may be mapped to "αβγδ" as per some candidate-specific mapping.

Currently, ATM pins (preferably 4 digit codes) provides the users the limited range of 10000 passwords (0000 to 9999) to choose for the authentication purpose. The present invention, if just using permutation on the 8-digit passcode provides the users much larger range of 40320 (=8!) combinations to choose from. If even 8 bit PIN is added to an OTP received first, the range of combinations users can choose from is 10^8 *8! = $4.032*10^{12}$. In

fact, much larger number of mappings are possible for a user to choose from. Including the dynamically changing parameters and more operators like min, max, conditional operators, etc. (which were generally simple to compute)in the functional mapping associated with the user, would further extensively increase the possibility to choose from, and thus making it much more difficult for the fraudsters to guess these mappings, and thus making the proposed solution much more secure.

As the candidate-specific mapping(and the associated parameters) are not transmitted over the communication channel and these mappings comprise of element-level operations/mappings so dynamic passcode easily computable (without necessarily using any software or hardware on the candidate side), the present invention is secure against the security attacks where the client/candidate side system/device or the information shared during authentication over the communication device or channel is once compromised or stolen or intercepted. As the passcode is dynamic for being dependent on media/multimedia transmitted (and possibly also on varying parameters associated with candidate-specific mapping), so it is not usable for authentication again and thus secure against the key-logging, snooping or shoulder surfing attacks. Also, even if sim-cloning or sim-swap attack once happens, the candidate-specific mapping is not known to the attacker, so this system is secure against these and other similar attacks also. The Trojan based attacks on smartphone applications as OTP generally received/generated on smartphone device is generally part of the OOB authentication, so the OTP (i.e. media/multimedia transmitted in simplest form) only gets known to the fraudster and not the dynamic passcode. Using element-level mappings/operations and other parameters (esp. varying data) in candidate-specific mapping makes it even much more difficult for the fraudster to guess the candidate-specific mapping (and associated parameters) even if very less likely event happens that both the bands that users user for authentication are compromised (data there is intercepted/monitored by fraudster) and user is completely unknown about this for long time. Using multimedia as the basis and not just the text makes it further harder for automated attacks to collect the information shared over communication channels and thus failing the fraudsters to succeed in compromising with the authentication system.

In one implementation, the authentication system and methods presented in this invention may be used in alone or in combination with other existing authentication methods and systems.

In some embodiments, the present invention be implemented as single factor authentication. In some embodiments, the present invention be implemented to facilitate multi-factor authentication. In some embodiments, the present invention be used in a single-band system (like one communication channel). In some embodiments, the present invention be used where communication is occurring across two or more channels.

Referring now to figure **1**, a networked implementation of a system**100** for providing secure authentication using dynamic passcode generated with candidate-specific mappingis illustrated, in accordance with an embodiment of the present subject matter.

Although the present invention is explained considering that the present invention is implemented as an authenticator **106**, it may be understood that the authenticator **106** may also be implemented in a variety of computing systems, such as a laptop computer, a desktop computer, a notebook, a workstation, a mainframe computer, a server, a network server, and the like. It will be understood that the authenticator **106** may be accessed by multiple users through one or more user/ electronic devices **102** (**102-1**, **102-2**...**102**-N devices), referred to as device **102** possessed by the user hereinafter, or applications residing on the user devices **102**. Examples of the candidate/user devices **102** may include, but are not limited to, a portable computer, a personal digital assistant, a handheld device, and a workstation. The devices **102** are communicatively coupled to the authenticator **106** through a network **104**.

In one implementation, the network **104** may be a wireless network, a wired network or a combination thereof. The network **104** can be implemented as one of the different types of networks, such as intranet, local area network (LAN), wide area network (WAN), the internet, and the like. The network **104** may either be a dedicated network or a shared network. The shared network represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like, to communicate with one another. Further, the network **104** may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, and the like.

In one implementation, the candidate may share one or more mapping(s) specific to oneself that would be used for generating the transformed/dynamic/first passcode (transformed media/multimedia) by either visiting the branch office and/or some secure communication media, the sharing of said candidate-specific mapping may be achieved by

means of a device **108** dedicated for submitting the candidate specific mapping which may be coupled to the authenticator **106** by means of a new or available network **106**.

In one implementation, the candidate shares the candidate-specific mapping by either visiting the branch office where said authenticator **106** is located, and/or via some secure communication media/ a new or said network **106**.

In one implementation, said candidate specific mapping is provided by said candidate using a dedicated device or selected from a set of pre-stored options provided by said user authentication system.

Referring now to figure **2**, an authenticator for authenticating a user is illustrated, in accordance with an embodiment of the present subject matter. In one implementation, the authenticator **106** may include at least one processor **202**, an interface **204**, and a memory **206**. The at least one processor **202** may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the at least one processor **202** is configured to fetch and execute computer-readable instructions that may be stored in the form of module/s **208** in the memory **206**.

The I/O interface **204** may be an input/output (I/O) interface and may include a variety of software and hardware interfaces, for example, a web interface, a graphical user interface, and the like. The I/O interface **204** may allow the authenticator **106** to interact with a user directly or through the user/ client devices **102**. Further, the I/O interface **204** may enable the authenticator **106** to communicate with other computing devices, such as web servers and external data servers (not shown). The I/O interface **204** can facilitate multiple communications within a wide variety of networks and protocol types, including wired networks, for example, LAN, cable, etc., and wireless networks, such as WLAN, cellular, or satellite. The I/O interface **204** may include one or more ports for connecting a number of devices to one another or to another server.

The memory **206** may include any computer-readable medium known in the art including, for example, volatile memory, such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes. The memory **206** may include modules **208** and database **218**.

The modules **208** include routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. In one implementation, the modules **208** may include a transmitter module **210**, a receiver module **212**, a passcode matching module **214**, and an authentication module **216**. The other modules (not shown) may include programs or coded instructions that supplement applications and functions of the authenticator**106**.

The database **218**, amongst other things, serves as a repository for storing data processed, received, and generated by one or more of the modules **208**. The database may be a specific database herein after referred to as candidate database **218** to specifically include store said candidate-specific mapping in a candidate database. The other data (not shown) may include data generated as a result of the execution of one or more modules in the other module (not shown). In one implementation, said candidate database also store other information associated with the user that may include but not limited to user identification details like user id, contact number, date of birth, mail address, residential address, etc. Further, said candidate database may also store the password/s associated (preferably in hashed form) with said candidate and/or set be said candidate.

In one implementation, an authenticator **106** for authenticating a user is disclosed. The authenticator **106** for authenticating a candidate comprises a transmitter module **210**, in responsive to detecting an access request, configured to transmit at least one media/multimedia; a receiver module **212** configured to receive at least one first passcode, wherein said first passcode is a transformed media/multimedia obtained from said media/multimedia transmitted; a passcode matching module **214** configured to generate at least one second passcode based on said candidate-specific mapping pre-stored in at least one candidate database associated with said candidate, and match said transformed media/multimedia with said second passcode generated; and an authentication module **216**, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate.

In one implementation, a system**100** for authenticating a candidate is disclosed. The system comprises an authenticator **106** including a transmitter module **210**, in responsive to detecting an access request, configured to transmit at least one media/multimedia; a receiver module **212** configured to receive at least one first passcode, wherein said first passcode is a transformed media/ multimedia obtained from said media/ multimedia transmitted; a passcode matching module **214** configured to generate at least one second passcode based on

said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database **218** associated with said candidate, and match said transformed media/multimedia with said second passcode generated; an authentication module **216**, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate; and at least one device **108** communicably coupled to said authenticator and configured to provide or enable selection of said candidate-specific mapping for storing in said candidate database, wherein said candidate-specific mapping are pre-stored and customizable.

In one implementation, the device **108** may be a computing system, such as a laptop computer, a desktop computer, a notebook, a workstation, a mainframe computer, a server, a network server, and the like.

In one implementation, said access request (or say, attempt to authenticate) is triggered by said user by transmitting at least one request to said authenticator, said request is preferably selected from at least a user identification number, biometric log in, opening an application pre-stored in a device possessed by said user, or any combination thereof.

In one implementation, the present invention enhances the security features of the existing authentication systems or provides a complete new authentication solution.

In one implementation, the device **108** configured to provide or enable selection of said candidate-specific mapping for storing in said candidate database.

In one implementation, said candidate database **218** is a distributed database.

In one implementation, said transformed media/multimedia comprises or based on said media/multimedia and at least one parameter selected from a group of parameters involving data associated with a current or past transaction, unvarying candidate-specific data like candidateID, varying data accessible to both said candidate and said authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

In one implementation, wherein said transformed media/multimedia is transmitted by said candidate.

In one implementation, said user authentication system authenticates said candidate specifically when said second passcode received from said user matches with said confirmation passcode generated.

In one implementation, the present invention may be used for validating the authenticity of claimed authenticating system or say web-server, like for protecting against

phishing attacks. The system provides both the media/multimedia content transmitted (initial code) and also the dynamic passcode generated using the initial code and candidate-specific mapping, for the user/candidate to validate if the dynamic passcode presented is the one expected. In some embodiments, the initial code is presented by the candidate/user to the authentication system and the system responds with the dynamic passcode generated using initial code and candidate-specific mapping. The authenticity of the system is confirmed if the dynamic passcode provided is same as the expected passcode.

Referring now to figure **3** and **4** illustrates a method for authenticating a user, and a method for storing candidate-specific mapping (and its associated parameters) in the candidate database, respectfully, in accordance with an embodiment of the present subject matter. The method may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, functions, etc., that perform particular functions or implement particular abstract data types. The method may also be practiced in a distributed computing environment where functions are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, computer executable instructions may be located in both local and remote computer storage media, including memory storage devices.

The order in which the method described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method or alternate methods. Additionally, individual blocks may be deleted from the method without departing from the protection scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof. However, for ease of explanation, in the embodiments described below, the method may be considered to be implemented in the above described authenticator **106**.

At block **302**, a request from a user/ candidate / device possessed by the user to get authenticated is received by the authenticator **106**. In responsive to detecting an attempt to authenticate, the authenticator/server **106** of the authentication system **100** generates at least one media/multimedia. The media/multimedia generated is transmitted to the device possessed or nearby the user.

At block **304**, after receiving the media/multimedia generated by the authenticator 106, the candidate generates the first passcode which is a transformed media/multimedia

based on specific mapping and its associated parameters. The candidate-specific parameters may be identifiable by the candidate-specific mapping functions that may be pre-stored in the candidate-database possessed by the authenticator or candidate database that may be distributed but coupled to the authenticator. The first passcode which is a transformed media/multimedia generated is then transmitted to the authenticator.

At block **306,** the authenticator 106in response to the receipt of the first passcode from the candidate/device possessed/used by the candidate, generates at least one second passcode based on said media/multimedia transmitted to the candidate and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate.

At block **308,** the authenticator 106after generation of plurality of second passcodes, matches the first passcode received with the plurality of second passcodes.

At block **310,** the authenticator 106 if after matching finds that the first passcode matches with at least one of the plurality of passcodes, the authenticator authenticates the candidate and provides the access.

As shown in figure **4**, the candidate have to pre-store the candidate-specific mapping functions in the authenticator.

At block **402**, the authenticator is configured to receive at least one candidate-specific mapping function from at least one dedicated device communicable coupled with the authenticator.

At block **404,** the candidate is allowed to customize or update the candidate-specific mapping(s) shared/fed or pre-stored in the authenticator.

At block **406**,the updated candidate-specific mapping(s) are stored/saved in the user database. The candidate database may be a distributed database each storing at least one piece of the candidate-specific mapping(s) received.

In one example, according to the present invention, the candidate may visit the authenticator (such as a bank server or an office server located at some location) and submit/share the mapping that may be used for the generation of dynamic passcodes. Some examples of the mapping(s) are provided in the above sections. The mappings may be pre-stored in the authenticator and are displayed when some candidate wish to select them for passcode generation. The mapping(s) may also be customized as per candidate's requirement or comfort. These candidate specific mapping(s) are associated with the candidate preferably not directly but using some anonymous identifiers and stored accordingly for security

purposes. Also, these mapping(s) may be stored in distributed databases. Each candidate-specific mapping may include several element-level mappings and different parameters for each of these mappings. In one example, the candidate-specific mappings are stored in pieces in the distributed database and when a candidate attempts to authenticate, the pieces of the mapping functions corresponding to said candidate (by preferably using anonymous identifiers associated with said candidate) are fetched from these distributed databases and combined to form the mapping(s) which is used for generation of the passcode by the authenticator.

A dedicated device 108 may be used for submitting/sharing the mapping(s)to the authenticator. The device may be a computer, tablet or phone communicable coupled to the authenticator and configured to provide the required interface to the user so as to easily share the mapping(s) with the authenticator. Further, the dedicated device may have an OCR means to feed the mapping function that may be in written form and brought by the user for submitting. The dedicated device may have camera and/or the audio I/O facility using which the user may feed the mapping(s) to the authenticator such as orally.

When the candidate request for authentication, the authenticator first checks for the present of the candidate in database. The candidate may request by sending a message (SMS) to the authenticator, or by clicking or tapping on an authenticator application installed in it. The candidate may send a candidate identification code to the authenticator as a request. The candidate may send the request using a device possessed by him/her. The candidate may even use the biometric trigger and send the scanned biometrics to the authenticator. The device may be mobile phone, computer, laptop, tablet, ATM machine and the like computing devices.

After the access request is received from the candidate, the authenticator generates a media or multimedia, such as an OTP, a sequence of randomly generated variables or alphabets or audios or images. The authenticator may also generate a multimedia file. The media or multimedia may be generated using techniques that are known now or developed in the future, like random number generator or a sequencer or image generator or audio generator, and the like already existing/future techniques. The media or multimedia generated is sent to the device possessed by the user.

When the candidate receives the media or multimedia from the authenticator, it modifies or transforms the media or multimedia to generate a dynamic passcode (the first passcode or the transformed media/multimedia). The candidate transforms the media or

multimedia based on the candidate-specific mapping (and its associated parameters) which may be already provided/shared with the authenticator as explained above. The transformed media or multimedia is computed using element level mappings and the parameters (as discussed above) that may be a part of the pre-shared or pre-stored candidate-specific mapping function at authenticator. The dynamic passcode (the first passcode or the transformed media/multimedia) is then sent to the authenticator.

As soon as the dynamic passcode (or the transformed media/multimedia) is received, the authenticator is configured to generate an authenticator passcode (second passcode / transformed passcode generated by the authenticator) based on the pre-stored candidate-specific mapping and the media or multimedia generated and transmitted to the candidate earlier. The authenticator may generate multiples passcodes based on the plurality of candidate-specific mappings pre-stored. The authenticator may generate passcodes by first retrieving the pieces of candidate-specific mappings stored in the distributed databases to form the candidate-specific mappings thereinafter these mappings may be used for generation of the multiple passcodes.

The authenticator, after generation of plurality of passcodes, matches the first passcode received from the candidate with the plurality of the authenticator passcodes generated by the authenticator. If at least one match is found in the mapping, the authentication of the candidate is successful or else the candidate is not authenticated.

In one implementation, the present invention may be used for number of application scenarios for strengthening the security by using a dynamic passcode instead of a static passcode. This system may be used in any scenario, where a server/authenticating authority can generate a one-time passcode (OTP) and make the same OTP available to the user/client side by some means such as but not limited to directly sending it to the user/client side or by synchronizing with a device on the user/client side. The user may then modify the OTP and sends the transformed passcode (or say, dynamic passcode) for authentication. The server/authenticating authority may use this dynamic passcode, received from the user and may compares with the expected passcode, and accordingly authenticates the user. The transformed passcode may be used in total or in partial along with other authenticating methods or information for enhancing the security.

In one implementation, the user or client side may be capable of obtaining the original media/multimedia from the server either by directly receiving through a communication channel or by synchronizing one's device with the server. The client side may be further

capable of receiving the original media/multimedia in a manner utilizable for the candidate and sending back the candidate's input (transformed media/multimedia) to the server.

In one implementation, the present invention may be used at ATM machine(s) which conveys a random passcode as communicated by the server or as generated in synchronization with the server, every time someone inserts a card into the machine. The random passcode may be conveyed as in text form or in image form (displaying the CAPTCHA images with random passcode embedded within) or in audio form or other multimedia form. The ATM may grant the usage rights to the user only after the user's input (dynamic passcode) matches with the second passcode generated at the server using the mapping specific to that particular user. In one such implementation, the ATM device ID and/or user's credentials may also be used as some input/seed for generating the initial random passcode generated by the server. Similar to an ATM, the proposed system can also be used at point of sales (PoS) and other similar systems.

In one implementation, the present invention may be used in scenarios where only single band/communication is available (like mobile banking, ATM etc., or even in cases similar to net-banking when personal devices not used for receiving/generating OTP for some reasons). A plurality of multimedia forms are transmitted (like displaying several CAPTCHA images) to the candidate, and candidate may randomly choose one of these multimedia forms to use as basis for generating the dynamic passcode (or say, first passcode) using candidate-specific mapping and then sending the dynamic passcode to the authentication system which compares the received passcode with the plurality of second passcodes generated using these plurality of multimedia forms transmitted and the candidate-specific mapping. In some implementation, the candidate may have already shared some information (like some specific image) as part of the candidate-specific mapping parameters, that which specific multimedia of the given several options need to be used for generating the first and second passcodes, and accordingly comparison is done for validating the authentication.

In one implementation, the present invention may be used for granting access to secure labs (or other premises/places where access to secure information is restricted to legitimate users only). The access control system device displays/provides the media/multimedia to the candidate attempting to access the lab/premises, and the transformed media/multimedia is then provided by the user. Only if the transformed passcode matches with the expected passcode (computed using the original media/multimedia initially provided

to the candidate and the candidate-specific mapping), the access is granted or restricted for that candidate.

Although implementations for methods and systems for secure authentication using dynamic passcode have been described in language specific to structural features and/or methods, it is to be understood that the appended claims are not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as examples of implementations for secure authentication using dynamic passcode.

WE CLAIM:

1. An authenticator **106** for authenticating a candidate, said authenticator comprising:

a transmitter module **210**, in responsive to detecting an access request, configured to transmit at least one media/multimedia;

a receiver module **212** configured to receive at least one first passcode, wherein said first passcode is a transformed media/multimedia obtained from said media/multimedia transmitted;

a passcode matching module **214** configured to:

generate at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate;

match said transformed media/multimedia with said second passcode generated;

an authentication module **216**, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate.

2. The authenticator as claimed in claim **1**, comprises at least one device **108** configured to provide or enable selection of said candidate-specific mapping for storing in said candidate database.

3. The authenticator as claimed in claim **1**, wherein said media/multimedia content comprises two or more elements, the elements are preferably selected from alpha numeric values, ASCII characters, regional language characters, symbols or some other form of information.

4. The authenticator as claimed in claim **1**, wherein said candidate-specific mapping is configured to generate at least one output, the output consists of two or more elements, and each element is independently based on at least one parameter selected from a group of parameters involving elements associated with said media/multimedia, data associated with a current or past transaction, unvarying data known to both said candidate and said authenticator like candidateID, varying data accessible to both said candidate and said

authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

5. The authenticator as claimed in claim **1**, wherein said candidate database **218** is a distributed database.

6. The authenticator as claimed in claim **1**, wherein said access request is triggered by said candidate by transmitting at least one request to said authenticator, said request is preferably selected from at least a candidate identification name/number/information, biometric log-in, opening an application pre-stored in a device possessed by said candidate, or any combination thereof.

7. The authenticator as claimed in claim **1**, wherein said transformed media/multimedia comprises or based on said media/multimedia and at least one parameter selected from a group of parameters involving data associated with a current or past transaction, unvarying candidate-specific data like candidateID, varying data accessible to both said candidate and said authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

8. The authenticator as claimed in claim**1**, wherein said first passscode is transmitted by said candidate.

9. A method for authenticating a candidate by an authenticator **106**, said method comprising:

transmitting **302**, in responsive to detecting an access request, at least one media/multimedia;

receiving **304,** at least one first passcode, wherein said first passcode is a transformed media/multimedia, wherein said transformed media/multimedia obtained from said media/multimedia transmitted;

generating **306,** at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate;

matching **308,** said transformed media/multimedia with said second passcode generated;

authenticating **310**, in responsive to the match of said transformed media/multimedia with said second passcode, said candidate.

10. The method as claimed in claim **10**, comprises providing or enabling, by at least one device, selection of said candidate-specific mapping for storing in said candidate database.

11. The method as claimed in claim **10**, wherein said media/multimedia content comprises two or more elements, the elements are preferably selected from alpha numeric values, ASCII characters, regional language characters, symbols or some other form of information.

12. The method as claimed in claim **10**, comprises generating at least one output, using said candidate-specific mapping, wherein the output consists of two or more elements, and each element is independently based on at least one parameter selected from a group of parameters involving elements associated with said media/multimedia, data associated with a current or past transaction, unvarying data known to both said candidate and said authenticator like candidateID, varying data accessible to both said candidate and said authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

13. The method as claimed in claim **10**, wherein said candidate database is a distributed database.

14. The method as claimed in claim **10**, wherein said access request is triggered by said candidate by transmitting at least one request to said authenticator, said request is preferably selected from at least a candidate identification name/number/information, biometric log-in, opening an application pre-stored in a device possessed by said candidate, or any combination thereof.

15. The method as claimed in claim **10**, wherein said transformed media/multimedia comprises or based on said media/multimedia and at least one parameter selected from a

group of parameters involving data associated with a current or past transaction, unvarying candidate-specific data like candidateID, varying data accessible to both said candidate and said authenticator like day, month, year, time, date, region related information when/where access is requested, or any combination thereof.

16. The method as claimed in claim **10**, wherein said first passcode is transmitted by said candidate.

17. A system **100** for authenticating a candidate, said system comprising:

an authenticator **106** comprising:

a transmitter module **210**, in responsive to detecting an access request, configured to transmit at least one media/multimedia;

a receiver module **212** configured to receive at least one first passcode, wherein said first passcode is a transformed media/multimedia obtained from said media/multimedia transmitted;

a passcode matching module **214** configured to:

generate at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database **218** associated with said candidate;

match said transformed media/multimedia with said second passcode generated;

an authentication module **216**, in responsive to the match of said transformed media/multimedia with said second passcode, authenticating said candidate; and

at least one device **108** communicably coupled to said authenticator and configured to provide or enable selection of said candidate-specific mapping for storing in said candidate database, wherein said candidate-specific mapping are pre-stored and customizable.

18. A computer-readable medium having stored therein a computer program that causes a computer to implement a method for authenticating a candidate, the computer program causing the computer to execute:

transmitting **302**, in responsive to detecting an access request, at least one media/multimedia;

receiving **304,** at least one first passcode, wherein said first passcode is a transformed media/multimedia, wherein said transformed media/multimedia obtained from said media/multimedia transmitted;

generating **306,** at least one second passcode based on said media/multimedia and a plurality of candidate-specific mapping pre-stored in at least one candidate database associated with said candidate;

matching **308,** said transformed media/multimedia with said second passcode generated;

authenticating **310**, in responsive to the match of said transformed media/multimedia with said second passcode, said candidate.

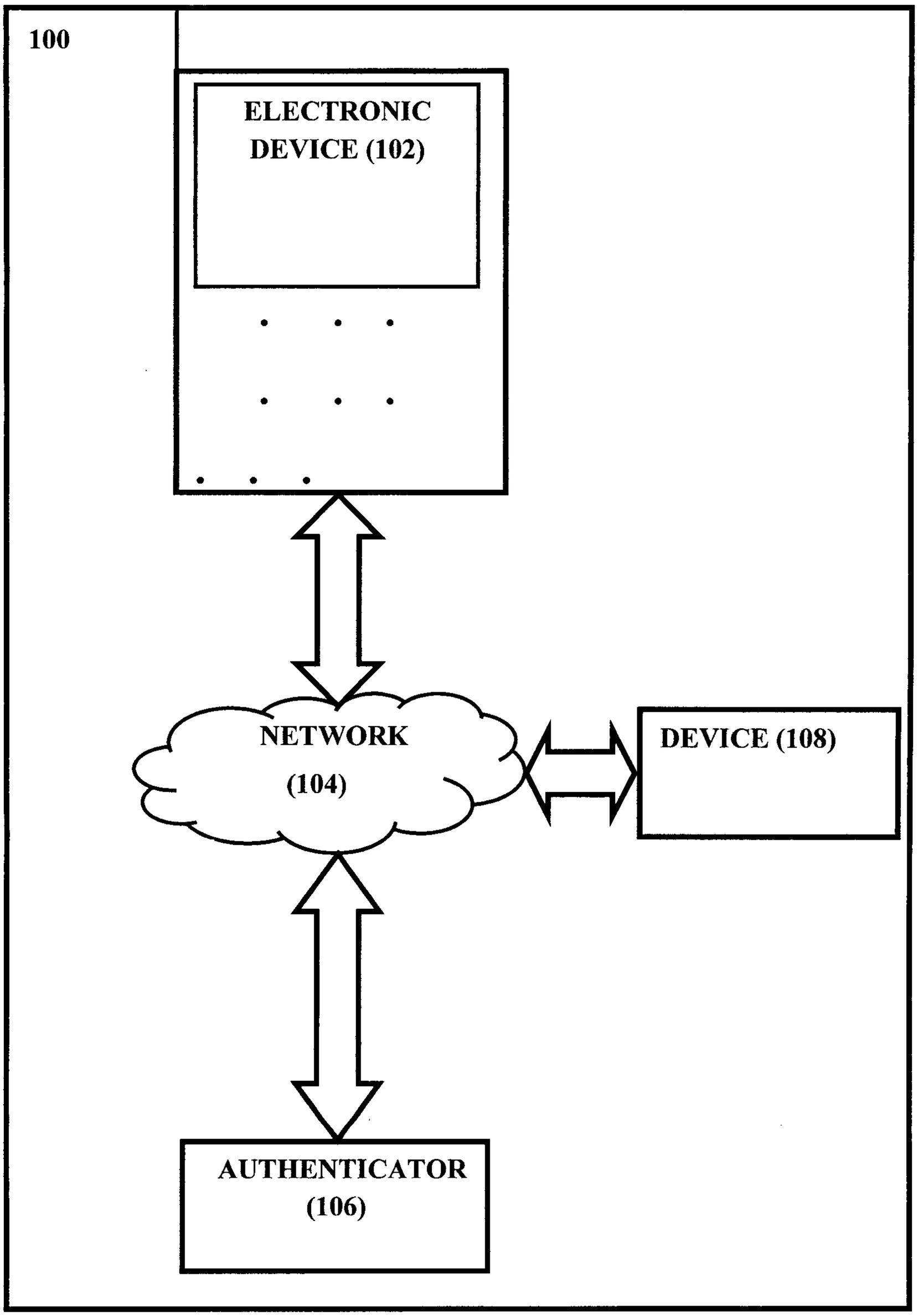

100
ELECTRONIC DEVICE (102)
NETWORK (104)
DEVICE (108)
AUTHENTICATOR (106)

FIGURE 1

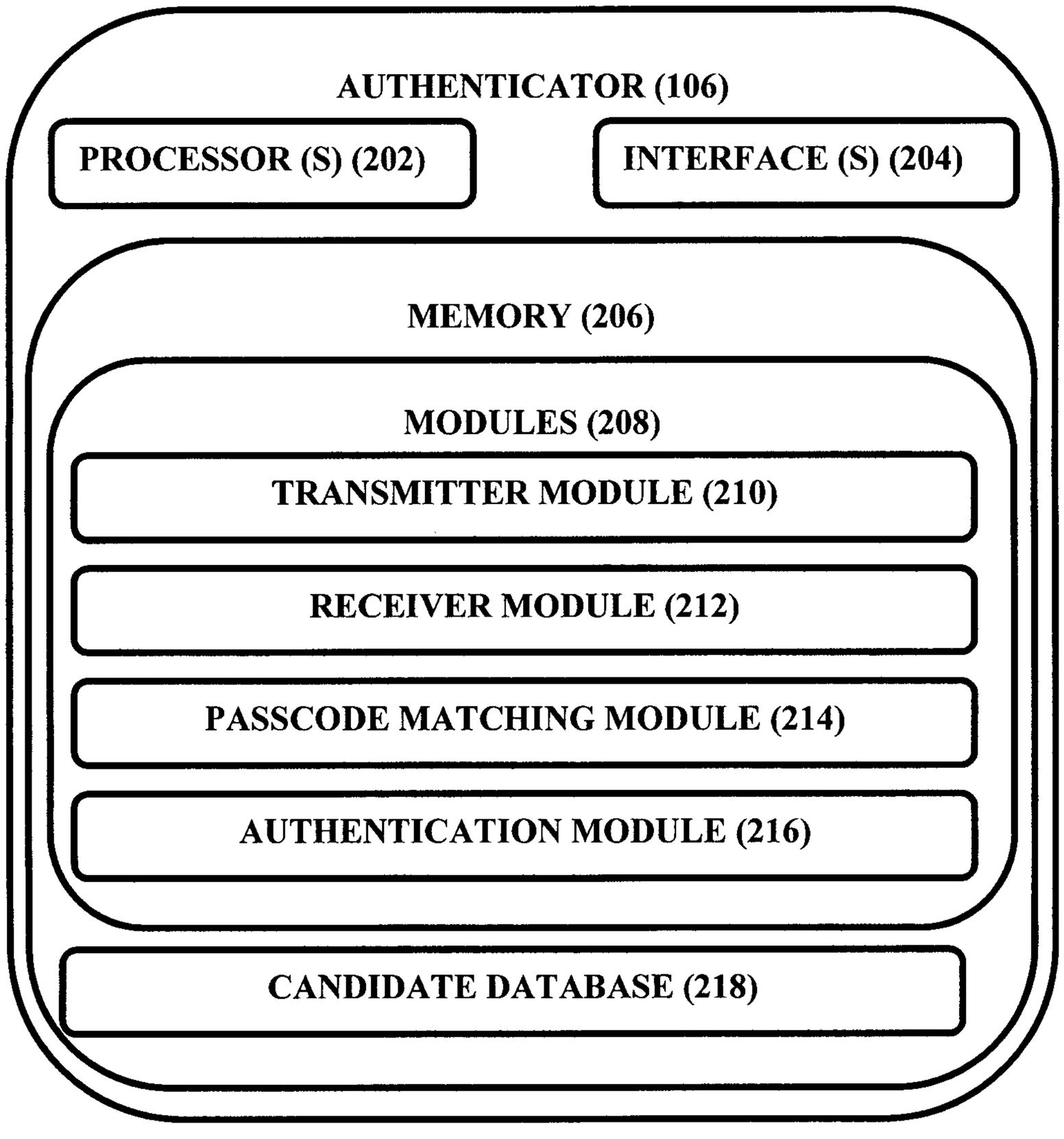

AUTHENTICATOR (106)
PROCESSOR (S) (202)
INTERFACE (S) (204)
MEMORY (206)
MODULES (208)
TRANSMITTER MODULE (210)
RECEIVER MODULE (212)
PASSCODE MATCHING MODULE (214)
AUTHENTICATION MODULE (216)
CANDIDATE DATABASE (218)

FIGURE 2

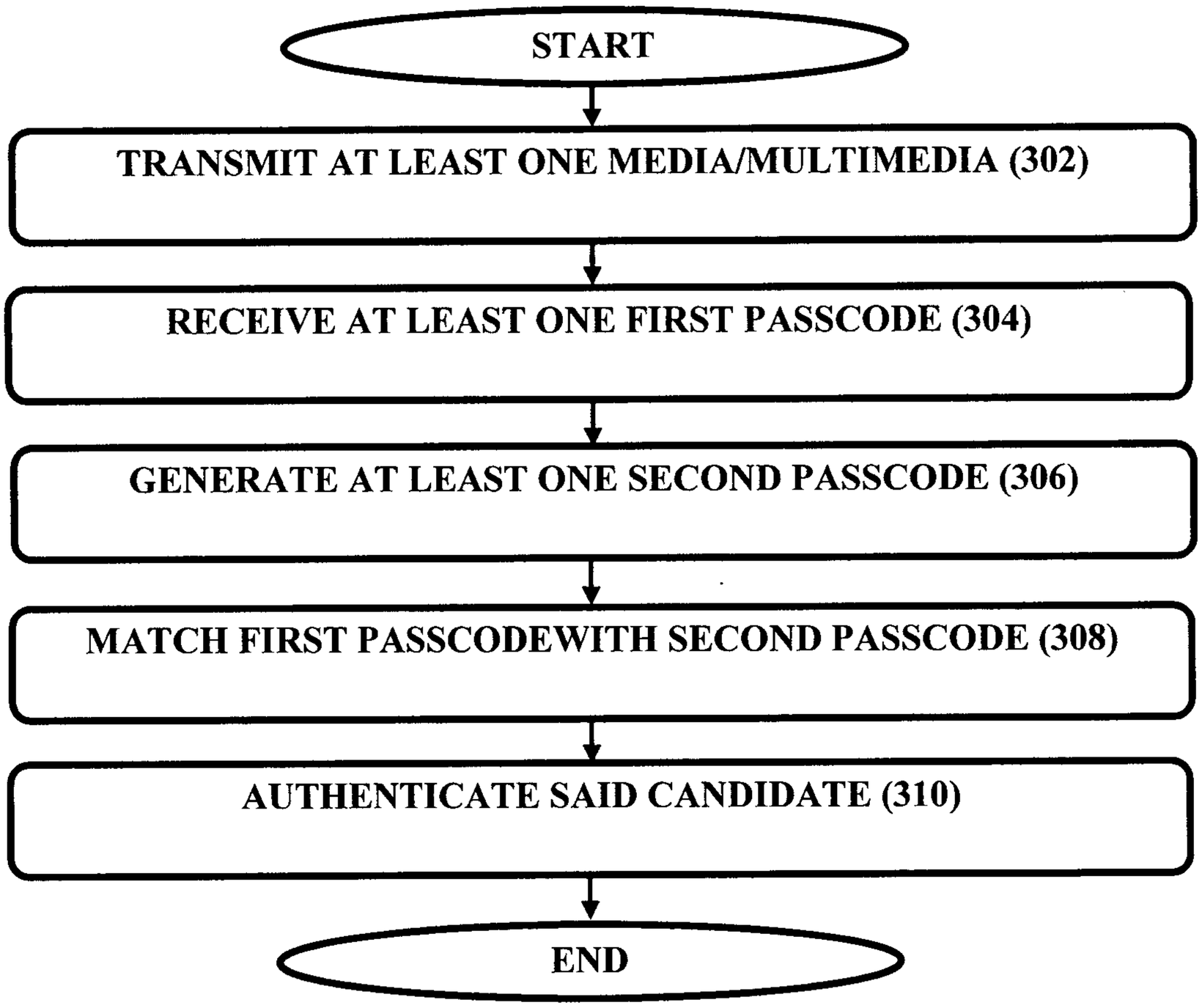


FIGURE 3

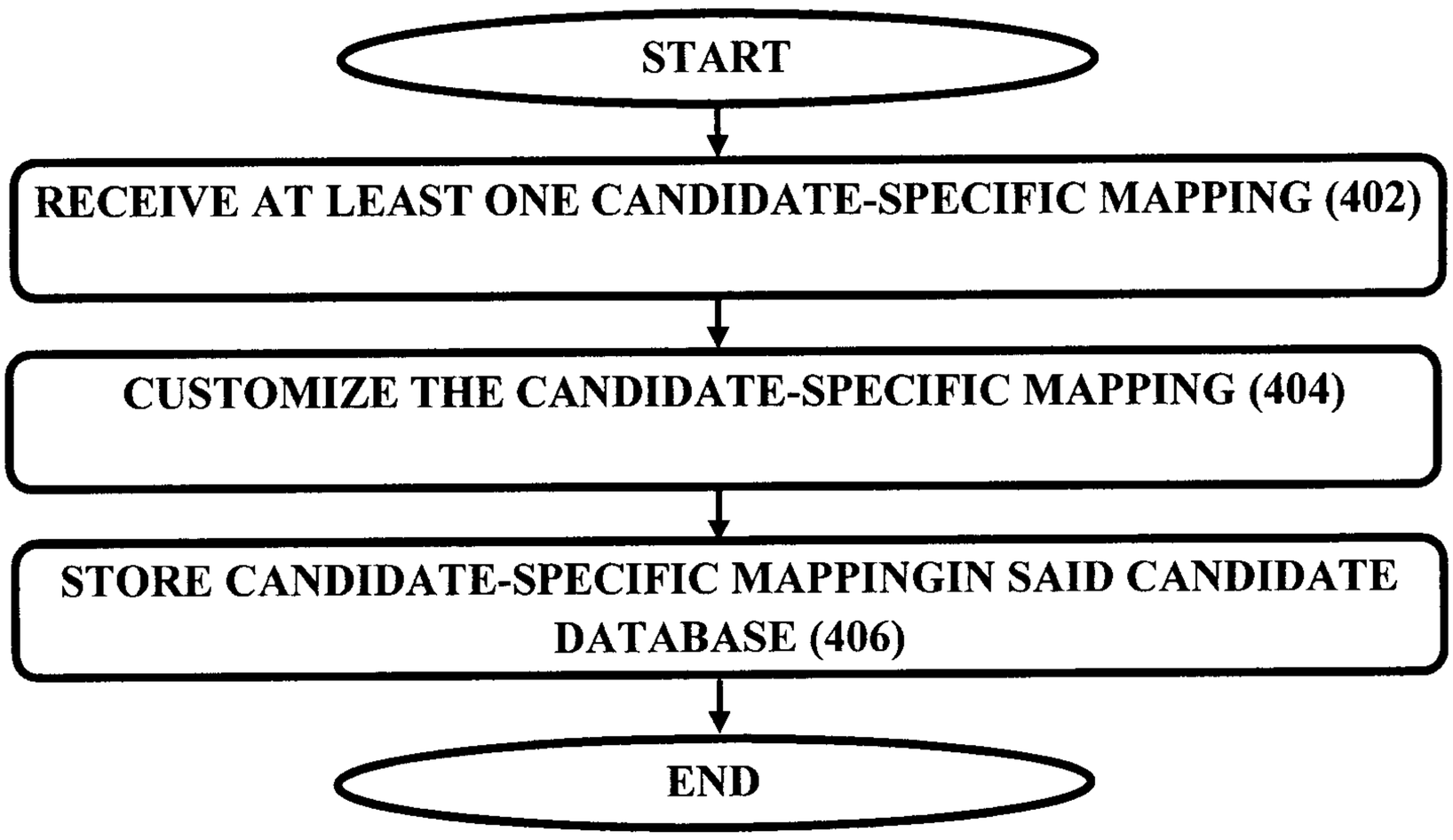
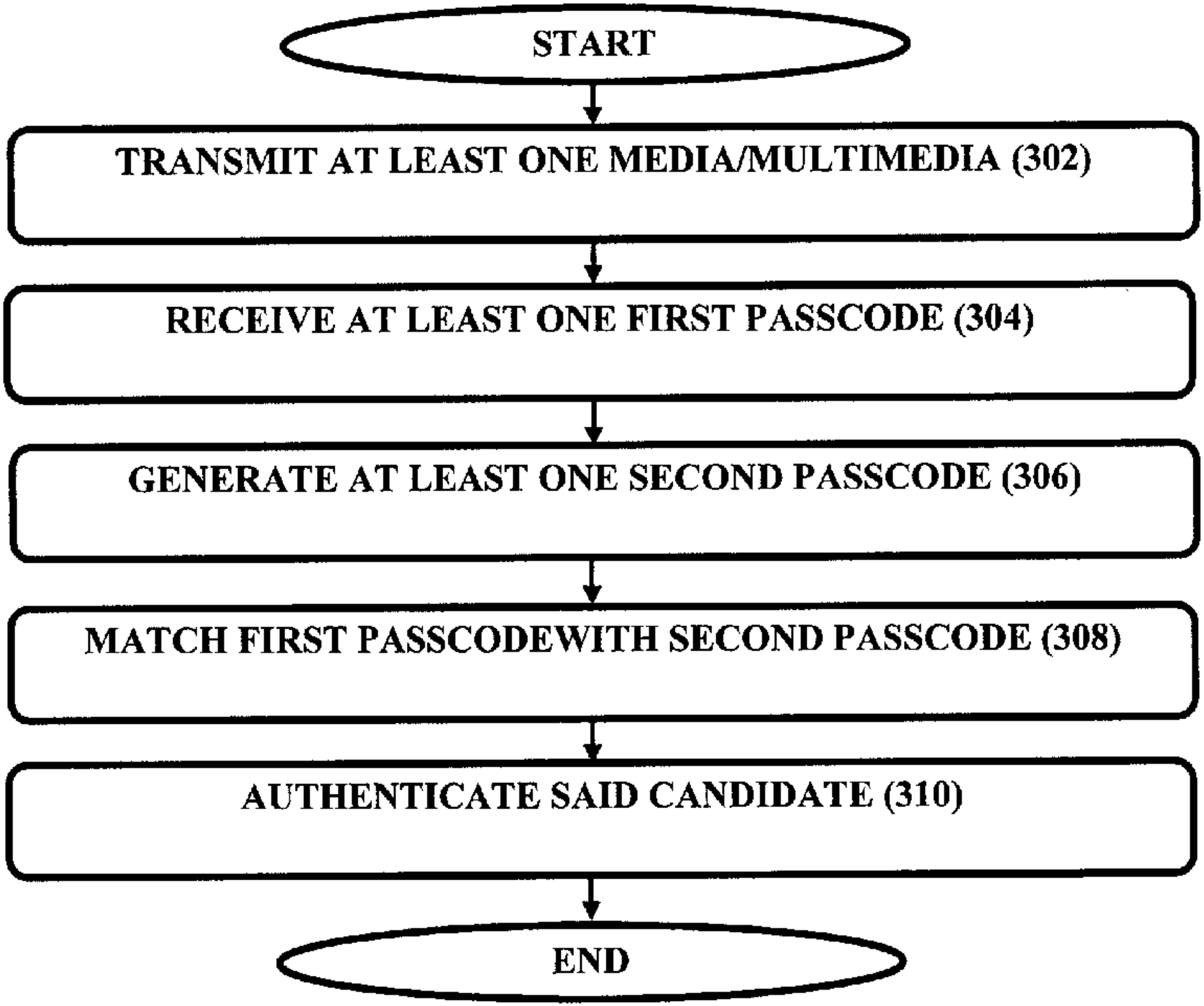


FIGURE 4


START
TRANSMIT AT LEAST ONE MEDIA/MULTIMEDIA (302)
RECEIVE AT LEAST ONE FIRST PASSCODE (304)
GENERATE AT LEAST ONE SECOND PASSCODE (306)
MATCH FIRST PASSCODEWITH SECOND PASSCODE (308)
AUTHENTICATE SAID CANDIDATE (310)
END