The following text is an excerpt from a patent application to USPTO authored and submitted by

***Akshay Sharma**.*

METHOD FOR ESTABLISHING GLOBAL UNIQUE ONLINE USER IDENTIFICATION SYSTEM WITH FACIAL RECOGNITION

ABSTRACT OF THE DISCLOSURE

The present invention comprises methods and systems for establishing a unique online identity of an individual or an Internet user globally, solely from his/her face without requiring any personal data, biographic data and/or government/institutional identity card(s)/document(s).

The system of the present invention can be used in at least three embodiments: for verifying if the facial image/video of the individual/user belongs to the individual (by social network(s) or other websites); uniquely identifying the online users for preventing online software piracy; as well as for preventing copyright infringement, violations of “terms of service”, illegal activities, etc. on the websites/web-services.

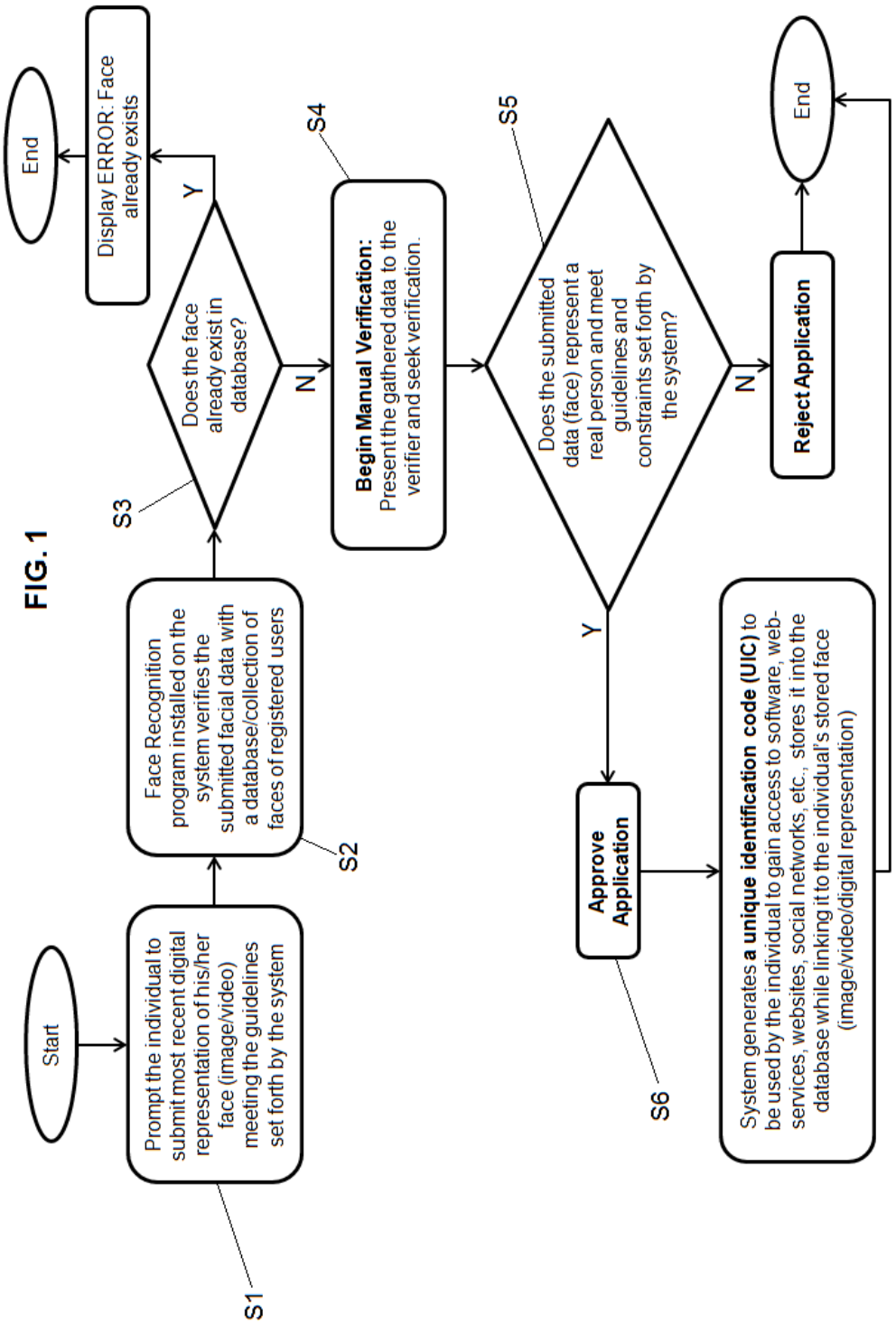
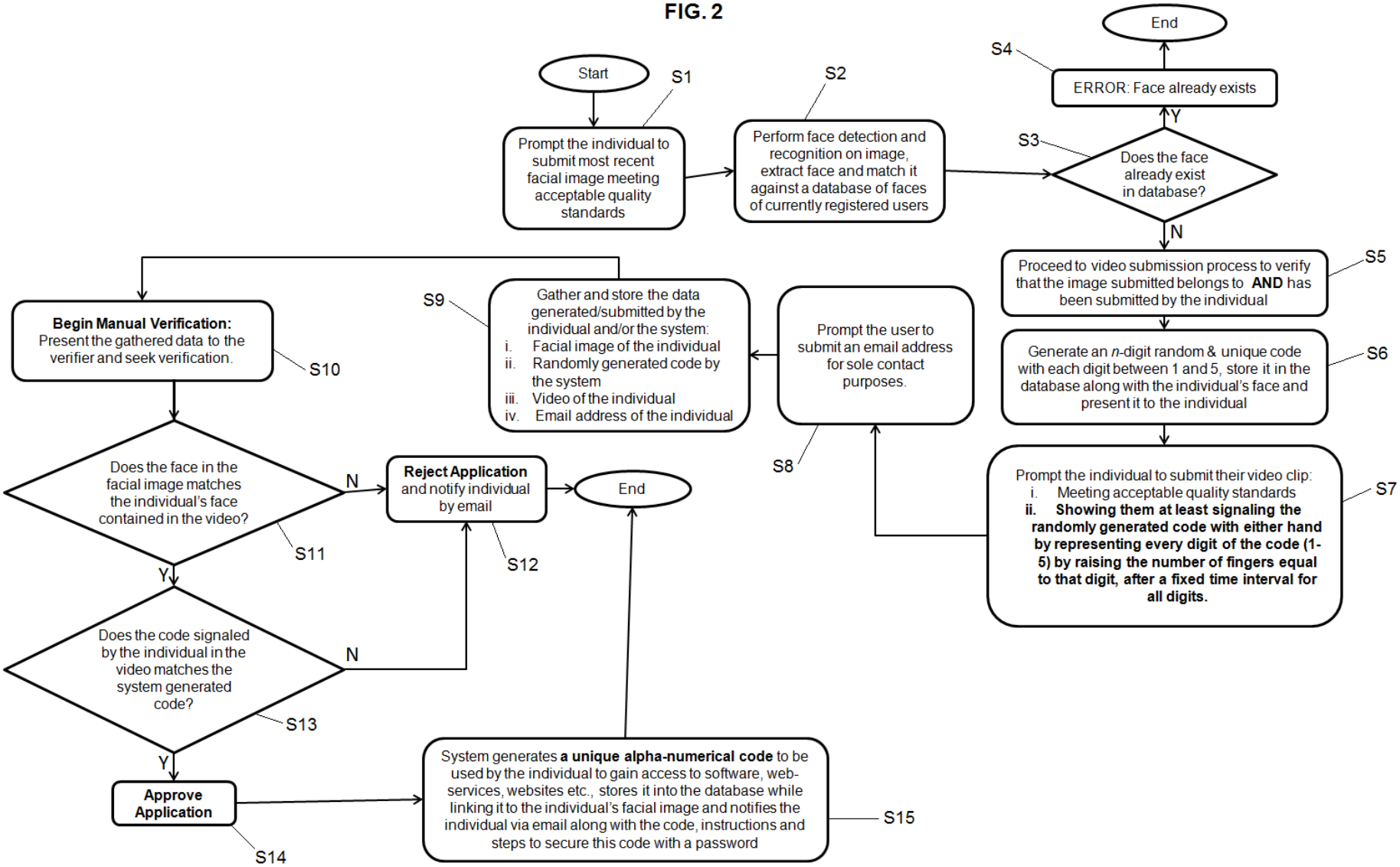


FIG. 1

FIG. 2



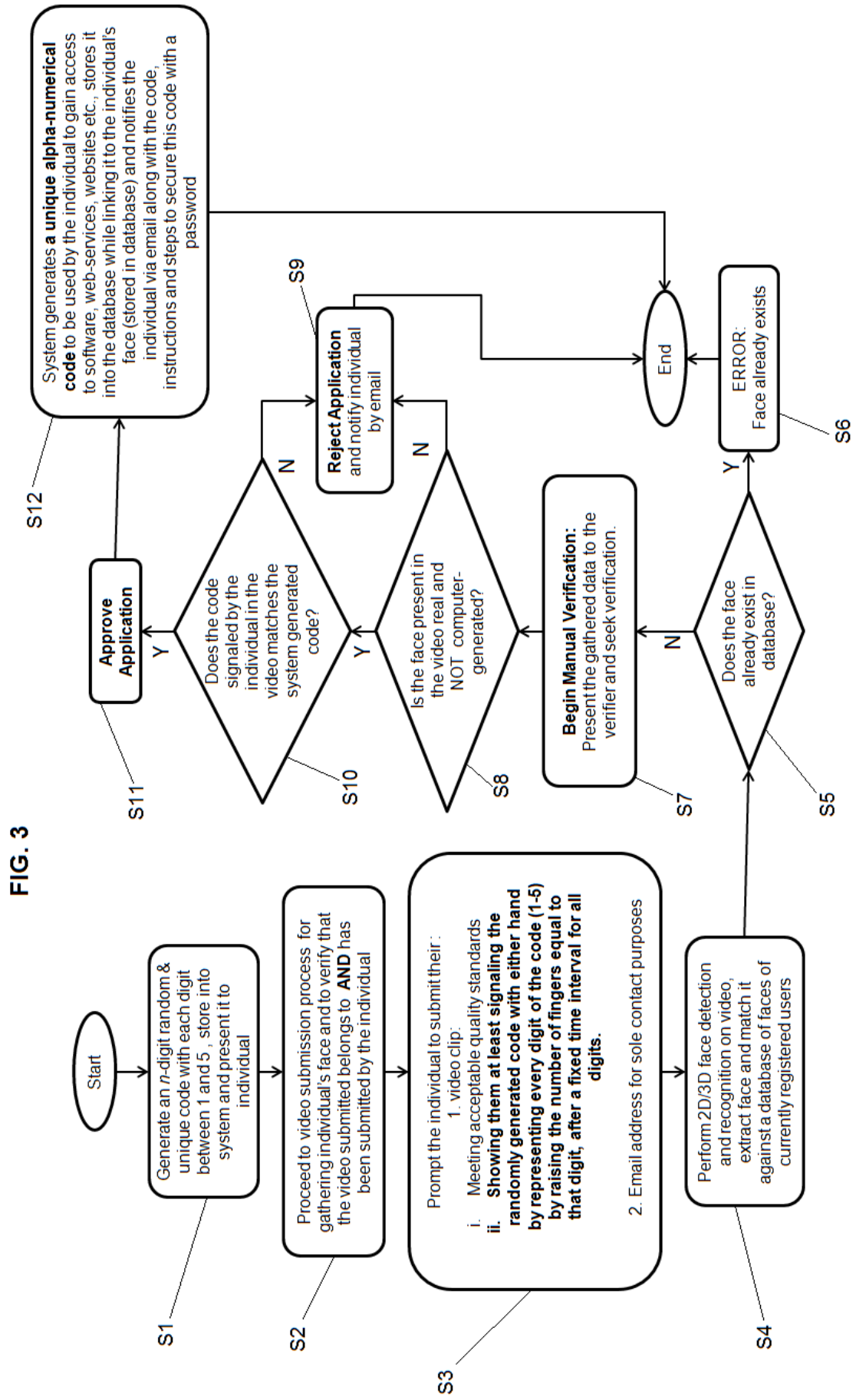


FIG. 3

FIG. 4 (a)

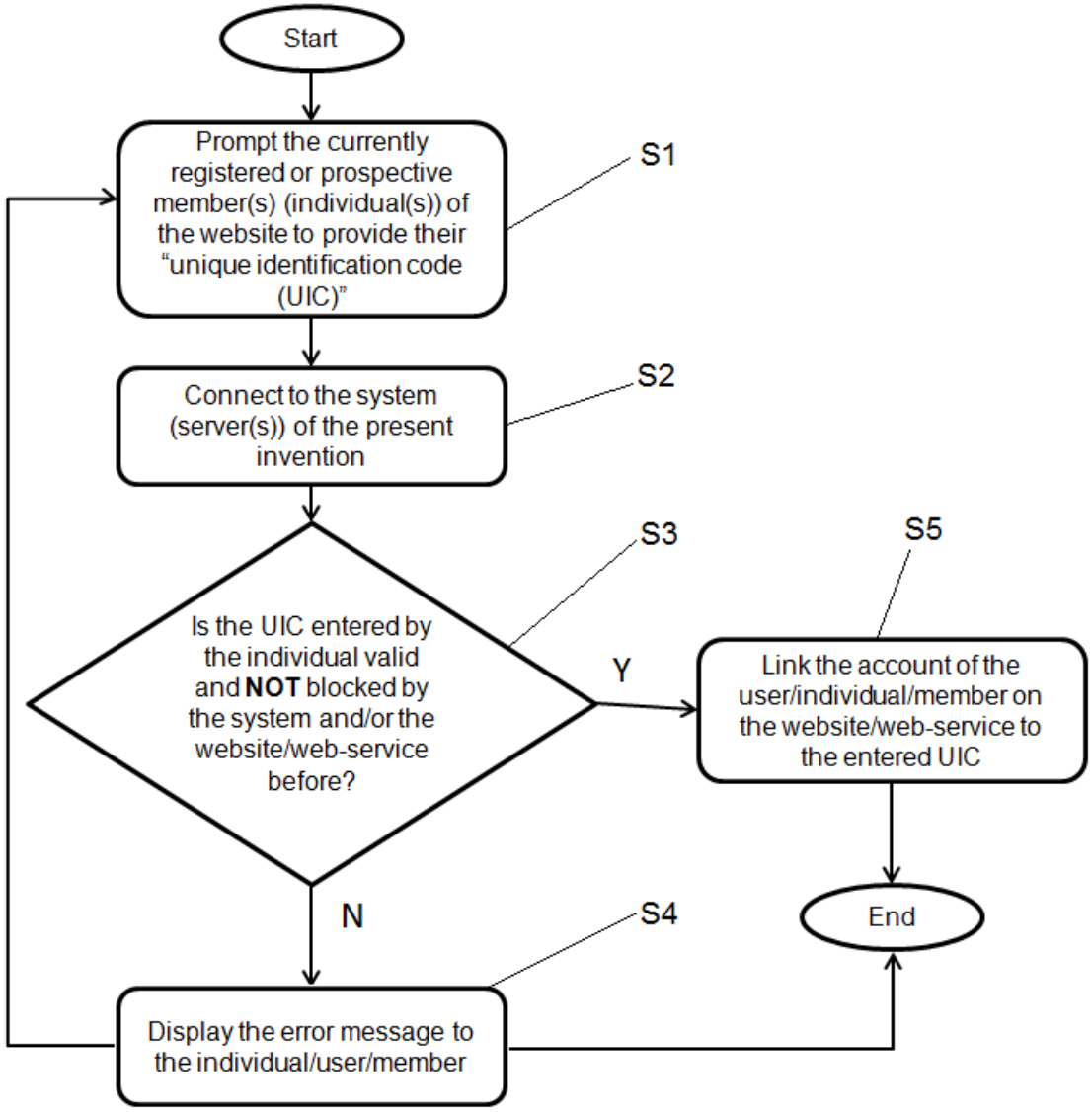
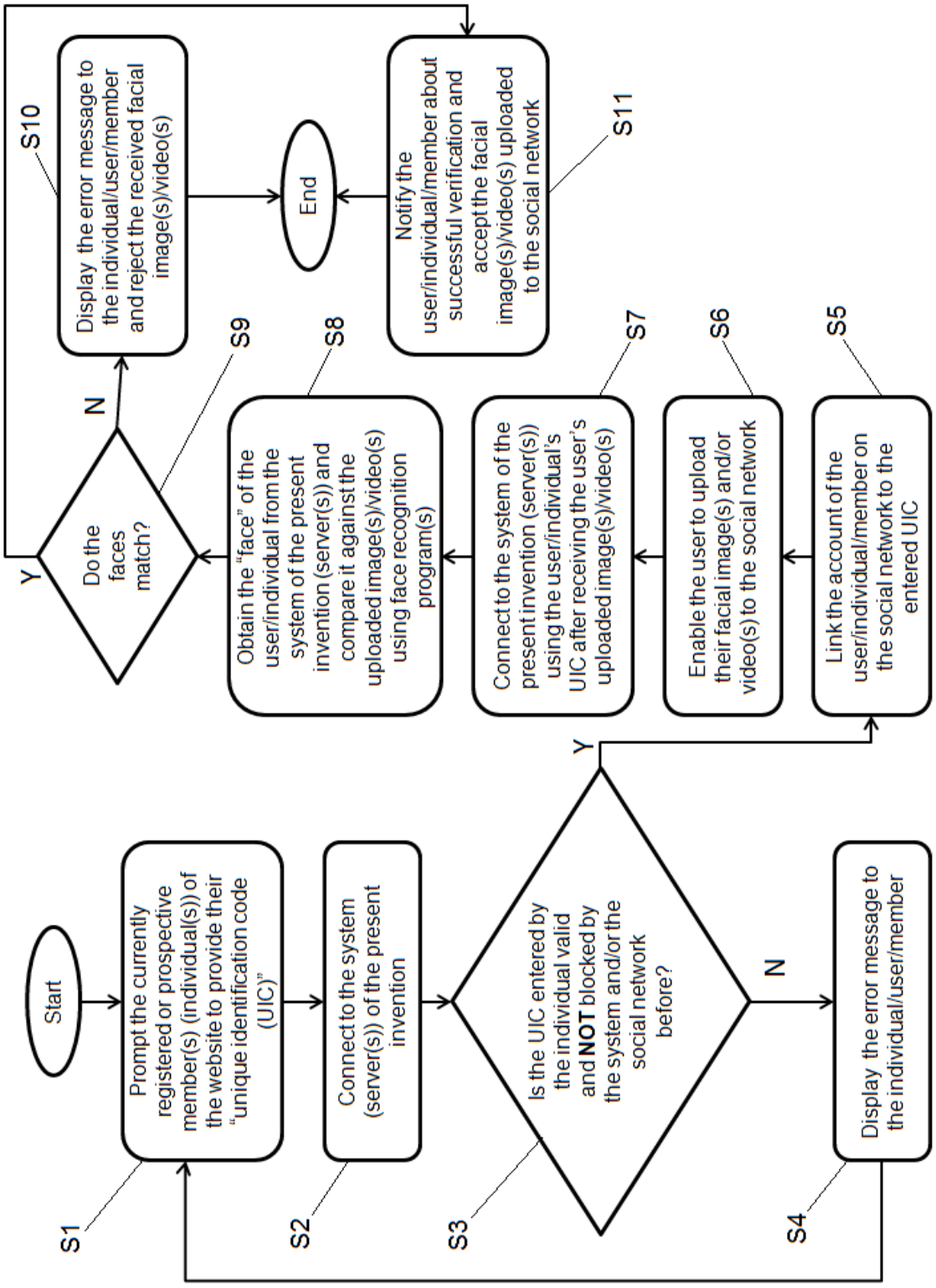


FIG. 4 (b)

FIG. 5



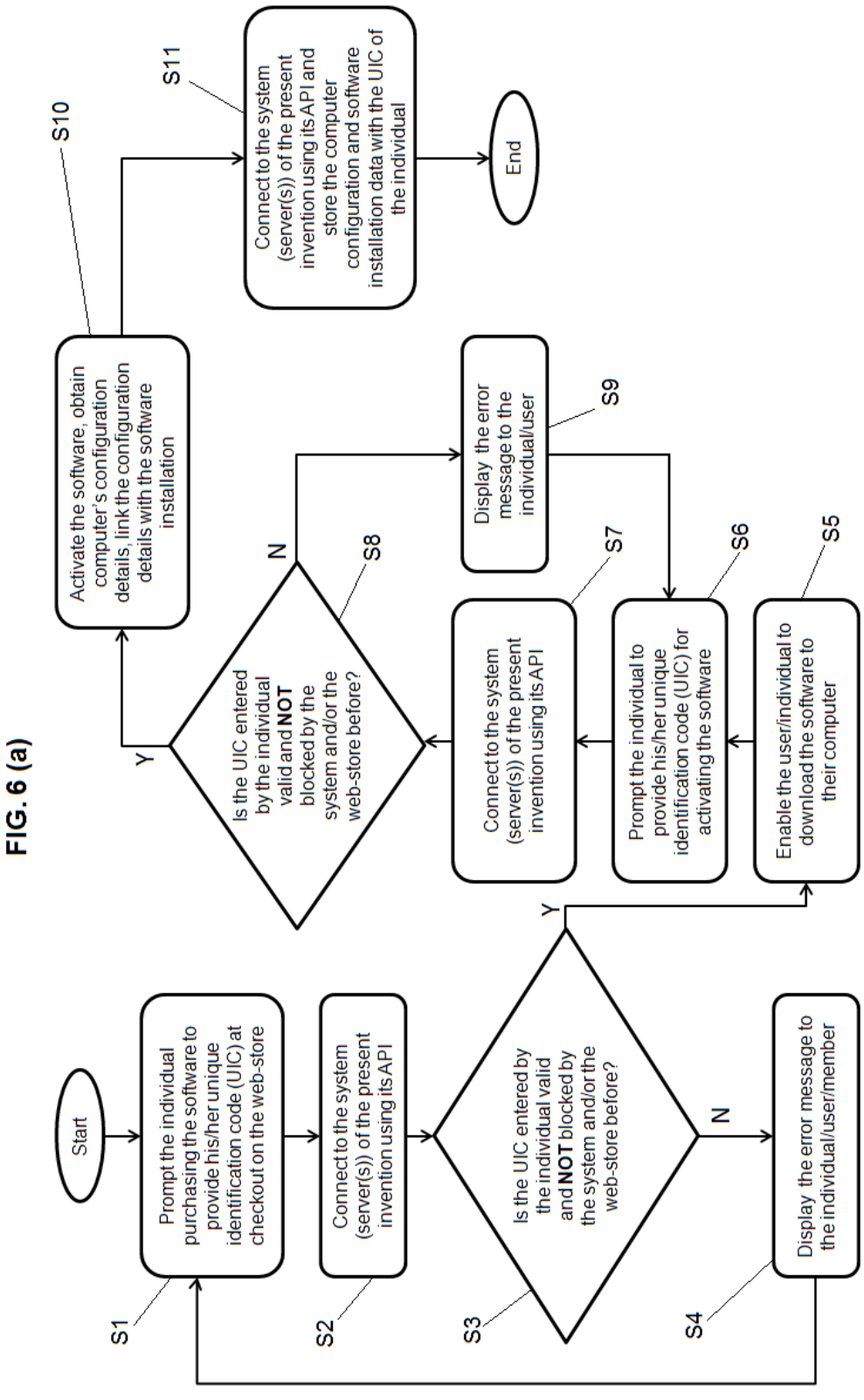


FIG. 6 (a)

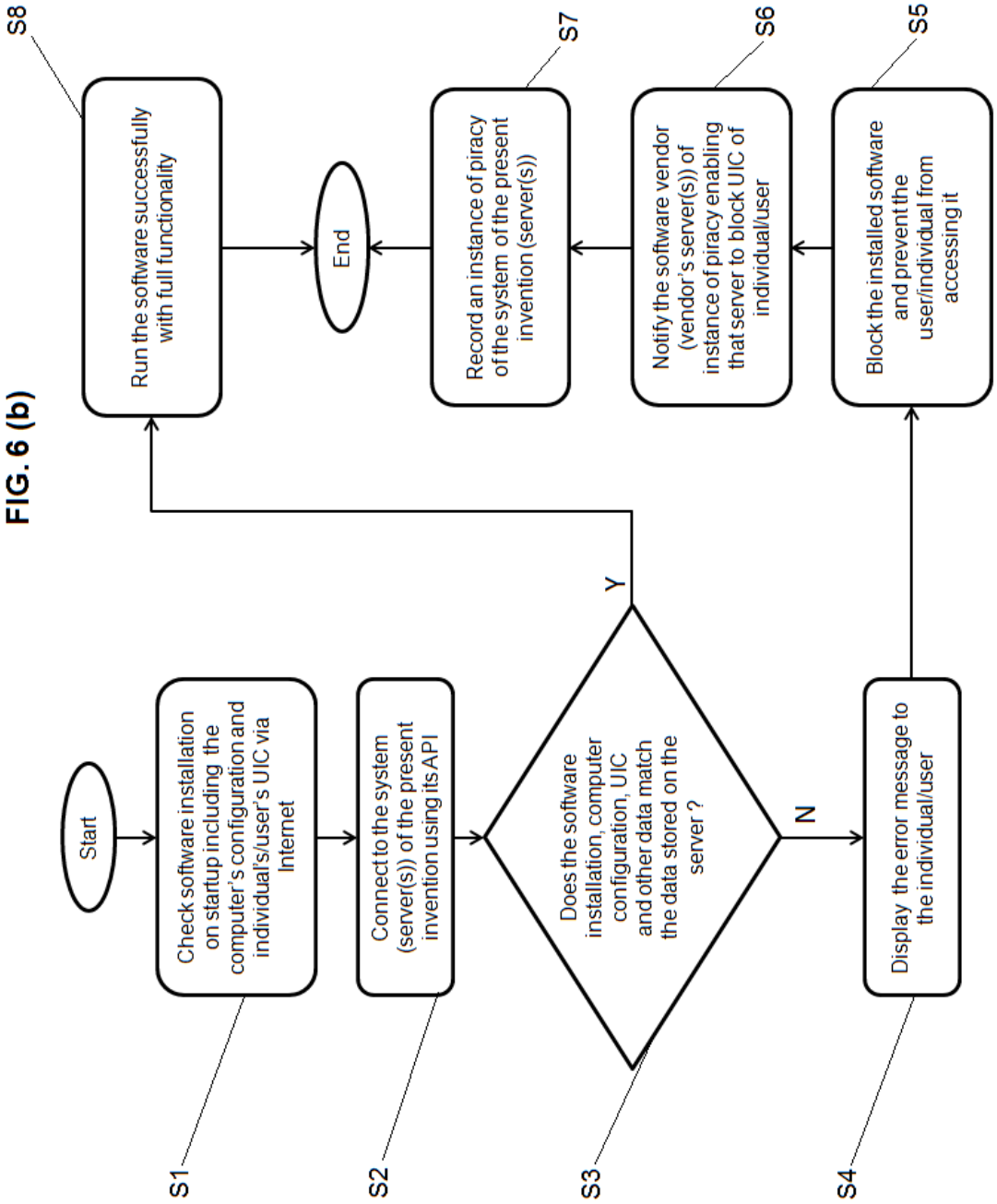


FIG. 6 (b)

BACKGROUND OF THE INVENTION

[0001] 1. TECHNICAL FIELD

[0002] The present invention is related to online identity verification systems and methods. In particular, methods and systems for establishing the unique online identities of Internet users/individuals.

[0003] 2. DESCRIPTION OF RELATED ART / PRIOR ART

[0004] In today's world, as much as the uses of Internet have expanded, so are the potential risks posed by some of its users; misusing it. Presently, there are no practical means to uniquely identify an individual online. The increasing rates of illegal activities like online software piracy, copyright infringements, violations of intellectual property rights, digital content theft and misrepresentation of one's identity (by the individual) can all be reasoned upon this fact. The problem arises for many online businesses, software firms and web-services/websites that have no means to identify its users and distinguish between safe (or honest) and "malicious" users/members/individuals (indulging in illegal activities) and block the "malicious" users. The only proper forms of identification are assumed to be the individual's/user's government issued identity documents along with the individual's/user's biographic data provided at his/her sole discretion. These forms of identification, if asked by one of the online businesses, software firms or websites, can also be illegally produced, digitally altered, replicated and misrepresented by the end-user/the individual. While, in reality, the end-users

or individuals are hesitant to provide their biographic data fearing that it can compromise their privacy or lead to a totalitarian society.

[0005] Presently, the most popular forms of online identification of an individual are the IP address of the individual's networking device(s) (for example, routers) and/or the digital device(s) (including but not limited to a computer, laptop, mobile phone, Personal Digital Assistant (PDA), tablet computer, camera, smart phone, or any other digital device(s) with similar/better capabilities) and the individual's email address, both of which can be easily be forged and/or reproduced and/or altered.

[0006] Only if every individual using the Internet for accessing web-services and/or websites and/or software etc. could be practically identified and the malicious users/individuals could be blocked, most cyber crimes would simply not exist.

[0007] Enhanced research and development in the field of computer vision are paving the way for new solutions like the ones discussed in the present disclosure to meet this challenge while ensuring convenience to the individual(s).

[0008] Patent application U.S. Patent 8024578 (filed: Jun 23, 2010 and issued: Sep 20, 2011, in the name of Armen Geosimonian) discloses process(es) that enable an individual to establish their online identity while requiring the individual's identity card(s) or document(s) issued by the

Government or some institution(s) and/or biographic data and the process is designed for mainly controlling online access to a study course.

[0009] The present invention, on contrary, is entirely different in terms of mechanism or otherwise, requires no biographic data from the individual and has entirely different embodiments as described in the following disclosure.

SUMMARY OF INVENTION

[0010] The objectives of the present invention are to establish unique online identities of individuals using the Internet, globally and; a system controlling the access of the individuals to web-services, software, websites etc. that make use of this system.

[0011] The present invention proposes a method to execute the above two tasks. The basis for establishment of the individual's identity being used in the present invention is solely the face of the individual and this does not include any of their biographical data. That is, the present invention transforms the individual's face (received by the system in form of an image and/or a video) into their unique identity without requiring the individual's personal data.

[0012] Firstly, in order to establish an individual's unique online identity and initiate the application process, the individual connects to the server/system and is prompted to submit the most recent digital representation of his/her face in the form of a facial image and/or a video from his/her digital device (including but not limited to a computer, laptop, mobile phone, Personal Digital Assistant (PDA), tablet

computer, camera, smart phone, or any other digital device(s) with similar/better capabilities) to the server, online. A face recognition program (2D and/or 3D) installed on the server detects and extracts the individual's face from the submitted data (image and/or the video) and matches it against a database and/or collection of faces of currently registered users/individuals within the system.

[0013] If the face already exists, the individual is instantly notified with an error message and the process ends. If the face does not already exist in the database, it must be ensured that the face belongs to the individual who submitted the facial image and that the individual is aware of and willingly submitting his/her digital facial representation, in order to prevent any individual from misusing the facial image (or video) of other individual(s) (for example, by using facial image of another person(s) and posses multiple identities which would also prevent another person(s) from registering with the system because of the verification process involving manual reviewing).

[0014] To ensure such a protection, individual is also asked to:

i. Either submit their video clip (either recorded live or pre-recorded) meeting the proposed guidelines set forth by the system (in case the user submitted the facial image prior to proceeding for manual verification) from their digital device (including but not limited to a computer, laptop, mobile phone, Personal Digital Assistant (PDA), tablet computer, camera, smart phone, or any other digital device(s) with similar/better capabilities) to the server, online.

ii. Or, simply asked to revise and resubmit the video meeting the guidelines set forth by the system, in case the submitted video does not meet them.

[0015] Later, the image and/or the video submitted are manually verified to ensure that the face submitted is real, not computer generated and the content (image and/or video) submitted by the indivudal adheres to the proposed guidelines for submission(s).

[0016] Upon manual verification and approval of the application, the system generates a code consisting of alphabets and/or digits and/or special characters either randomly or based on the cryptographic hash of the submitted content, stores this code into the database while linking it to the individual's submitted face and notifies the individual/user of this generated code that acts as their "unique identification code (UIC)". This "unique identification code (UIC)" is used by the individual(s) to access various websites, web-services, software, etc.

[0017] Irrespective of the process followed, the objective of the present invention remains the same: establishment of unique identity without requiring any biographic or institutional/governmental issued document(s)/data.

[0018] The individual's "face" being used in the present invention as the basis of unique identification (code/UIC) along with the manual verification, prevents the registered individual to register again with the system and hence it is assured that every individual can have only one (unique) identity.

[0019] However, due to the nature of faces and the effects of ageing on faces, there can be significant changes in the face of an individual over a given period of time. This means that a currently registered individual might be able to register again into the system and receive a separate unique identification code (UIC) such that the individual now has more than one identity. To prevent this situation, the present invention consists of a identity renewal process in which the currently registered individuals in the system, after a given period of time are required submit a new and recent digital representation of their face in form of an image/video along with their current unique identification code (UIC) (to ensure that the user is registered) and repeat the verification process. The unique identification code (UIC) submitted along with the latest facial image/video helps the system in comparing the current face linked to the unique identification code (UIC) to the newly submitted digital face representation (image/video), overlook minor changes caused over the given period of time, add the new face to the individual's collection of face(s) stored on the system and/or set the individual's "most recent" face from the current/old face stored on the system to the newly submitted face.

BRIEF DESCRIPTION OF DRAWINGS

[0020] While the appended claim(s) set forth the features of the present invention with particularity, the invention, together with its objects and advantages, may be best understood from the detailed description taken in conjunction with the accompanying drawings of which:

[0021] FIG. 1 is the flowchart representing the basic process of the present invention;

[0022] FIG. 2 is the flowchart of a proposed method of practically executing the process represented in **FIG. 1**;

[0023] **FIG. 3** is the flowchart of another proposed method of practically executing the process represented in **FIG. 1**;

[0024] **FIG. 4 (a)** is the flowchart describing the process of one of the embodiments of the present invention representing how the system (of the invention) can be utilized by a website or a web-service to identify and deter its members (the individuals) from indulging in copyright infringement / violation of Terms of Service of the website/web-service.

[0025] **FIG. 4 (b)**, related to **FIG. 4 (a)** is the flowchart describing the process of denying an individual/member access to the website/web-service by in an event of online piracy or copyright infringement or violation of Terms of Service of the website/web-service, by the website/web-service owners and/or auditors and/or robots.

[0026] **FIG. 5** is the flowchart of another embodiment of the present invention describing how a social network can verify whether the facial image(s)/video(s) uploaded to the social network by the individual/member belongs to the individual/member or not.

[0027] **FIG. 6 (a)** is the flowchart of another embodiment of the present invention describing how the system can be integrated within software to prevent online software piracy.

[0028] **FIG. 6 (b)** is the flowchart related to **FIG. 6 (a)** representing the flow of actions taken upon every start up of the software and in an event of software piracy.

DESCRIPTION OF PREFERRED EMBODIMENTS

[0029] In one embodiment of the present invention, various websites or web-services hosting files, games, videos, ebooks, music, media or any other digital

content can make use of the present invention or system disclosed herein to prevent the violation of copyrights and intellectual property rights.

[0030] Referring to **FIG. 4 (a),** the website or the web-service requires all of its current or prospective members (individuals) to register with the system in the present invention provide their “unique identification code (UIC)” generated by the method(s) used by the present invention (step **S1**) and links the individual’s account on the website/web-service to this “code” using the system’s API (Application Programming Interface) after verifying that the UIC entered by the user/individual is valid (steps **S2, S3, S4 and S5)**.

[0031] Later, In case the individual violates the website’s terms of service, indulges in copyright infringement and/or intellectual property piracy etc. (as represented by **FIG. 4 (b)**) by, for example, uploading copyrighted material to the website/web-service and sharing it illegally or otherwise, the website or the web-service can block the individual’s account by blocking his “unique identification code (UIC)” from accessing the website/web-service again (step **S2**) either by using an automated auditing system and/or by manually auditing the individual/user accounts on their servers for copyrighted infringement or so. In such a case, the individual gets completely blocked out of the website/web-service because of the individual’s unique identification code (UIC) that can neither be altered nor not be regenerated because of the registration process of the present invention as discussed in the summary.

[0032] In another embodiment of the present invention, the system can be used by social networks to ensure that the individual’s account created on the social network:

i. is that of a real person, and

ii. has real facial images belonging to the person.

[0033] Additionally, this embodiment can also help in distinguishing between the real account(s)/profile(s) of public dignitaries, figures, celebrities or VIPs and the ones created by posers representing fraudulent profile(s)/account(s) of the dignitaries and misleading the public.

[0034] Referring to **FIG. 5** the social networking service/website requires all its current/prospective members (individuals) to register with the system of the present invention and link their social networking accounts to their "unique identification code (UIC)" (steps **S1,S2,S3,S4 and S5**). The social network can then connect to the system (mostly a server or a group of servers) using the system's API (Application Programming Interface) and gain access to the individual's "face" stored in the system by using his/her "unique identification code (UIC)" (steps **S7 and S8**). Furthermore, the facial image(s)/video(s) uploaded by the user on the social network can be compared against the one(s) stored on the system that have been already verified using facial recognition programs or so and it can be instantly determined whether the facial image uploaded by the individual (member) to the social network is real and/or belongs to the user or not (steps **S9, S10 and S11**).

[0035] Further, in another embodiment of the present invention, the system can be used by the software vendors (sellers, companies and firms) to prevent online software piracy of their product(s). In this embodiment, the software vendor integrates the system into their software product and/or marketplace (web-store) by using the system's API (Application Programming Interface) which provides access

to the system and also enables the software vendor to protect the software product(s) by providing necessary protection tools. Referring to **FIG. 6 (a),** the individual purchasing the software is prompted to enter his/her unique identification code (UIC) while purchasing the software online at the web-store (step **S1**); verifies whether the UIC entered is valid by connecting to the system (steps **S2** and **S3**) and enables the individual/user to proceed to download the software upon successful verification (step **S5**). Once downloaded and launched for installation, the individual/user is prompted for the UIC again for activating the software (step **S6**) on his/her computer. The system's API verifies whether the individual's unique identification code (UIC) is valid (steps **S7** and **S8**) and upon successful verification activates the software (step **S10**).

[0036] The software once activated on a computer, links the Operating System (OS) and/or hardware and/or computer configuration (for example, the "user name" of the individual's account on his/her computer) of the computer (unique to that computer) to the individual's unique identification code (UIC) via Internet (step **S10**). The system (mainly server(s)) receives and maintains records of the configuration, UIC and user's details (step **S11**).

[0037] Referring to **FIG. 6 (b),** upon every startup or run, the software connects to the system via the Internet to ensure that the individual's unique identification code (UIC) is valid and not been blocked or disabled (steps **S1** and **S2**). If the computer's configuration saved on server, matches the computer's configuration (step **S3**), the software runs successfully (step **S8**). In an instance of piracy in which the individual illegally copies the software onto another computer, the software:

i. detects a mismatch in the new computer's configuration; connects to the Internet and blocks the individual's unique identification code (UIC) (step **S6**) while recording the instance of piracy for this unique identification code (UIC) (step **S7**). Once blocked the unique identification code (UIC) of the individual becomes invalid and cannot be used anywhere else (on the software vendor's website / anywhere else in general) unless unblocked by the system or system administrator.

ii. fails to run on the new computer/device because of a mismatch of hardware configuration and blocks the installed software (step **S5**) (by, for example, deleting installation and activation files) .

[0038] Hence, the individual that legally purchased the software would not consider indulging in online software piracy as doing so will get his UIC (required to access other software, websites, social networks, web-services etc) permanently blocked either on the (main) system or the software vendor's web-store or both. Also, even if the software is copied or pirated, it would not be able to function on a computer other than the individual's computer who purchased it because of a different overall configuration of the new computer.

What is claimed is:

1. A method and a system for establishing unique online identity of the individual(s) comprising:

a system receiving a digital representation of the individual's face in the form of an image and/or a video submitted by the individual from a digital device; verifying if the face already exists on the system using a face recognition program/algorithm and sending back an error message if the face exists; otherwise manually verifying the submitted

data for ensuring it meets the proposed guidelines set forth by the system; system generating a unique code called “unique identification code” or UIC of the individual, consisting of alphabets and/or numbers and/or special characters either randomly or based on cryptographic hash of the individual’s face and/or submitted data, upon a successful verification; assigning this UIC to the individual’s face (facial data) present on the system to establish the unique identity of the individual.

2. Method of Claim 1, wherein a user or an individual or a member represents any person in general or a person using the Internet or a person registered with the system or otherwise.
3. Method of Claim 1, wherein the system or the system of the present invention refers to the entire system implementing the process of the present invention and comprising a server or group of servers performing at least data processing, verification and storage tasks for the present invention.
4. Method of Claim 1, wherein the term: “digital device” essentially includes but is not limited to a computer, laptop, mobile phone, Personal Digital Assistant (PDA), tablet computer, camera, smart phone, or any other digital device(s) with similar/better capabilities.
5. Method of Claim 1, wherein the “submitted data” comprises the digital representation of the individual’s face in form of a facial video and/or facial image.

* * * * *