



US012469411B2

(12) **United States Patent**  
**Forte et al.**

(10) **Patent No.: US 12,469,411 B2**  
(45) **Date of Patent: Nov. 11, 2025**

(54) **CONTENT ENCRYPTION AND IN-PLACE  
DECRYPTION USING VISUALLY ENCODED  
CIPHERTEXT**

(71) Applicant: **Cyphlens LLC**, Albany, NY (US)  
(72) Inventors: **Andrea G. Forte**, Brooklyn, NY (US);  
**Rocky Motwani**, New York, NY (US)  
(73) Assignee: **Cyphlens LLC**  
(\* ) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 246 days.

(21) Appl. No.: **18/369,214**  
(22) Filed: **Sep. 18, 2023**

(65) **Prior Publication Data**  
US 2024/0005820 A1 Jan. 4, 2024

**Related U.S. Application Data**  
(63) Continuation-in-part of application No. 18/140,626,  
filed on Apr. 28, 2023, which is a continuation-in-part  
(Continued)

(51) **Int. Cl.**  
**G09C 5/00** (2006.01)  
**G06F 21/62** (2013.01)  
(Continued)

(52) **U.S. Cl.**  
CPC ..... **G09C 5/00** (2013.01); **G06F 21/6245**  
(2013.01); **G06F 21/64** (2013.01); **H04L**  
**9/3236** (2013.01)

(58) **Field of Classification Search**  
CPC ..... G09C 5/00; G06F 21/6245; G06F 21/64;  
G06F 21/36; H04L 9/3236;  
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,588,414 B2 11/2013 Ishii  
8,924,712 B2 \* 12/2014 Varadarajan ..... H04W 12/06  
713/155

(Continued)

FOREIGN PATENT DOCUMENTS

CN 107248135 A 10/2017  
WO 2014005736 A1 1/2014

OTHER PUBLICATIONS

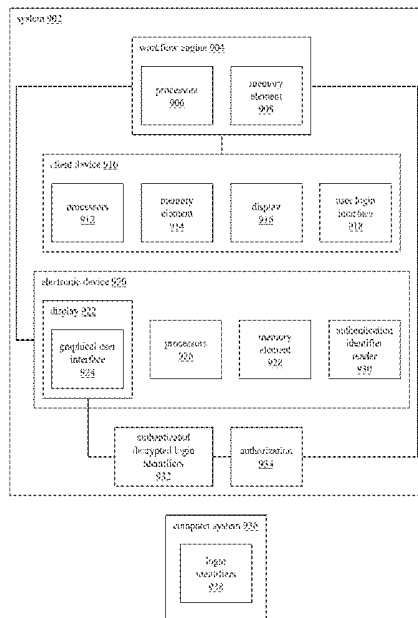
US 9,213,854 B2, 12/2015, Koo (withdrawn)  
(Continued)

*Primary Examiner* — Michael R Vaughan  
(74) *Attorney, Agent, or Firm* — Gearhart Law LLC

(57) **ABSTRACT**

A system for bidirectional two-factor remote user authentication includes a workflow engine comprising one or more processors and at least one memory element for storing instructions. The system further includes a client device with one or more processors, a display, and a user login interface. The workflow engine generates and encrypts one or more login identifiers, which is visually encoded as an authentication image and displayed on the terminal's display. An electronic device, also connected to the workflow engine, includes a password, a display with a graphical user interface, one or more processors, and at least one memory element. The device's authentication identifier reader decrypts the one or more login identifiers from the authentication image and compares it with the password to determine a match. Upon a match, the device transmits an authorization for the login request to the workflow engine.

**21 Claims, 13 Drawing Sheets**



**Related U.S. Application Data**

of application No. 17/715,055, filed on Apr. 7, 2022, now Pat. No. 11,676,515, which is a continuation of application No. 16/272,117, filed on Feb. 11, 2019, now Pat. No. 11,335,214.

(51) **Int. Cl.**

**G06F 21/64** (2013.01)  
**H04L 9/32** (2006.01)

(58) **Field of Classification Search**

CPC ..... H04L 2209/34; H04L 9/14; H04L 9/3226; H04L 9/3247; H04L 9/40; H04L 9/50  
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,135,489 B2 9/2015 Zhang  
9,183,677 B2 11/2015 Harple et al.  
9,230,148 B2 1/2016 Zhang  
9,251,366 B2 2/2016 Forte et al.  
9,330,272 B2 5/2016 Koo  
9,396,310 B2 7/2016 de los Reyes  
9,426,149 B2\* 8/2016 Wang ..... G06F 21/35  
9,571,785 B2 2/2017 Farrell  
9,893,890 B2 2/2018 Melzer  
9,948,659 B2 4/2018 Harple et al.  
10,325,101 B2 6/2019 Dow  
10,694,074 B2 6/2020 Chen  
10,706,161 B2 7/2020 Engel  
10,740,584 B2 8/2020 Ebrahimi  
10,747,868 B2 8/2020 Bock  
10,943,225 B2 3/2021 Flurschein  
11,057,214 B2 7/2021 Kim  
11,140,138 B2 10/2021 Li  
2009/0129591 A1 5/2009 Hayes  
2010/0074443 A1\* 3/2010 Ishii ..... H04N 1/32272  
380/243  
2013/0254858 A1\* 9/2013 Giardina ..... G06F 21/42  
726/7

2015/0090791 A1\* 4/2015 Zhang ..... G06K 7/1417  
235/462.04  
2015/0090792 A1\* 4/2015 Zhang ..... G06K 7/1417  
235/462.04  
2015/0178721 A1\* 6/2015 Pandiarajan ..... G06K 19/06112  
705/64  
2015/0295715 A1 10/2015 Melzer  
2015/0296170 A1\* 10/2015 Farrell ..... G06V 40/172  
386/254  
2015/0356306 A1 12/2015 Carter  
2016/0191506 A1\* 6/2016 Wang ..... H04L 63/18  
726/7  
2017/0032573 A1\* 2/2017 Dow ..... G06F 21/606  
2017/0140144 A1\* 5/2017 Bock ..... G06F 21/40  
2017/0161506 A1 6/2017 Gates  
2017/0257358 A1\* 9/2017 Ebrahimi ..... H04L 9/3236  
2018/0040164 A1 2/2018 Newman  
2018/0167215 A1 6/2018 Melzer  
2018/0204206 A1\* 7/2018 Flurschein ..... G06K 19/06037  
2018/0234588 A1\* 8/2018 Chen ..... H04L 51/52  
2018/0307883 A1\* 10/2018 Ebrahimi ..... G06K 7/1439  
2019/0149335 A1\* 5/2019 Kim ..... G09C 5/00  
713/155  
2019/0228140 A1\* 7/2019 Arroyo ..... G06V 40/1365  
2020/0028826 A1\* 1/2020 Li ..... G06T 7/136  
2021/0117565 A1\* 4/2021 Ringler ..... G06F 21/602  
2025/0088504 A1\* 3/2025 Liu ..... H04L 63/0838  
2025/0165974 A1\* 5/2025 Forte ..... G06Q 20/3274

OTHER PUBLICATIONS

M. Eminagaoglu, E. Cini, G. Sert and D. Zor, "A Two-Factor Authentication System with QR Codes for Web and Mobile Applications," 2014 Fifth International Conference on Emerging Security Technologies, Alcalá de Henares, Spain, 2014, pp. 105-112 (Year: 2014).\*  
F. Xu, S. Han, Y. Wang, J. Zhang and Y. Li, "QRToken: Unifying Authentication Framework to Protect User Online Identity," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 2015, pp. 368-373 (Year: 2015).\*

\* cited by examiner

*High-level pipeline used to convert data to visually encoded ciphertext*

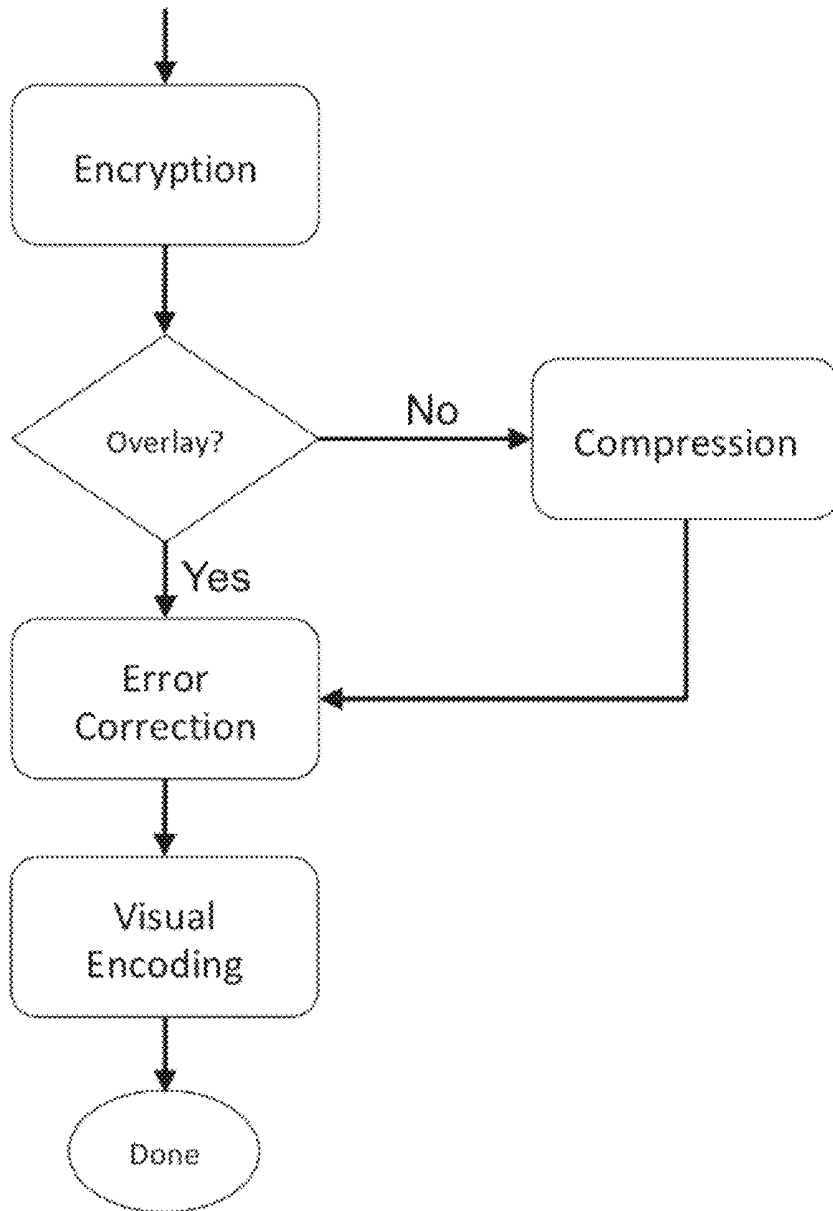


FIG. 1

Non-overlaid content

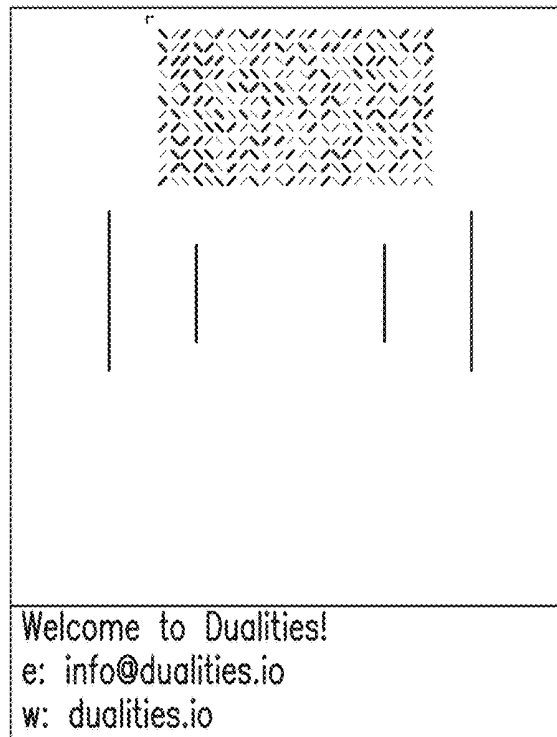


FIG.2A

Overlaid content

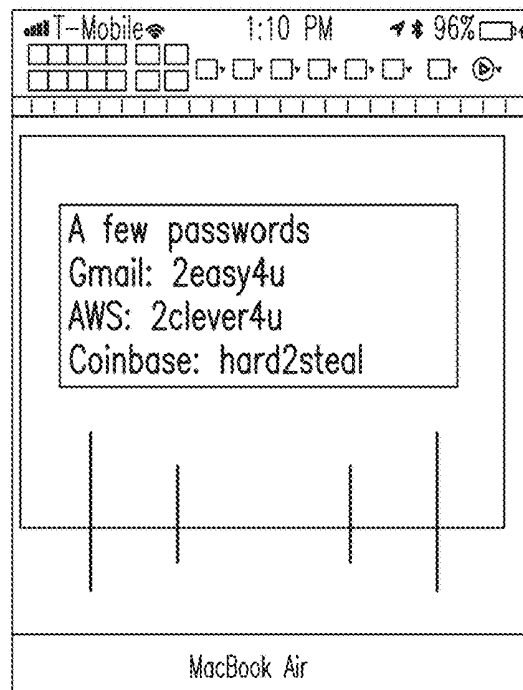


FIG.2B

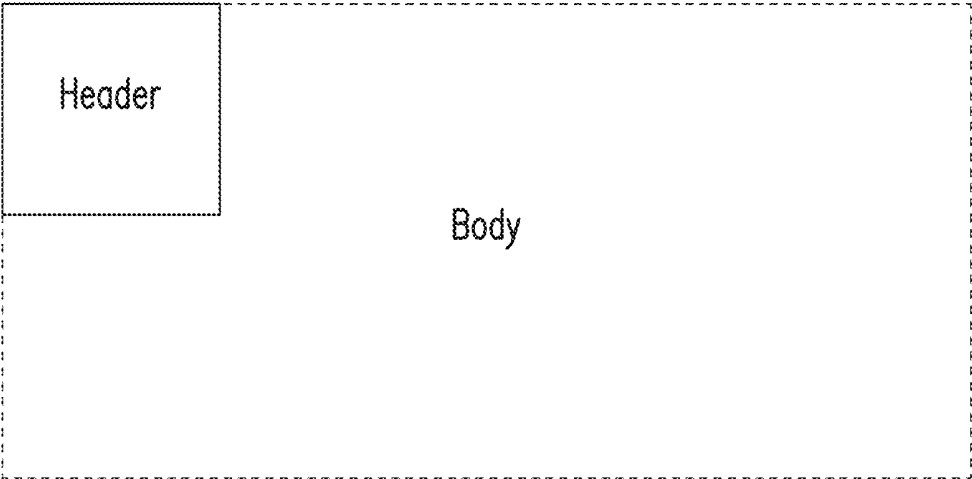


FIG.3

*Example of Transaction Summary with PIN*

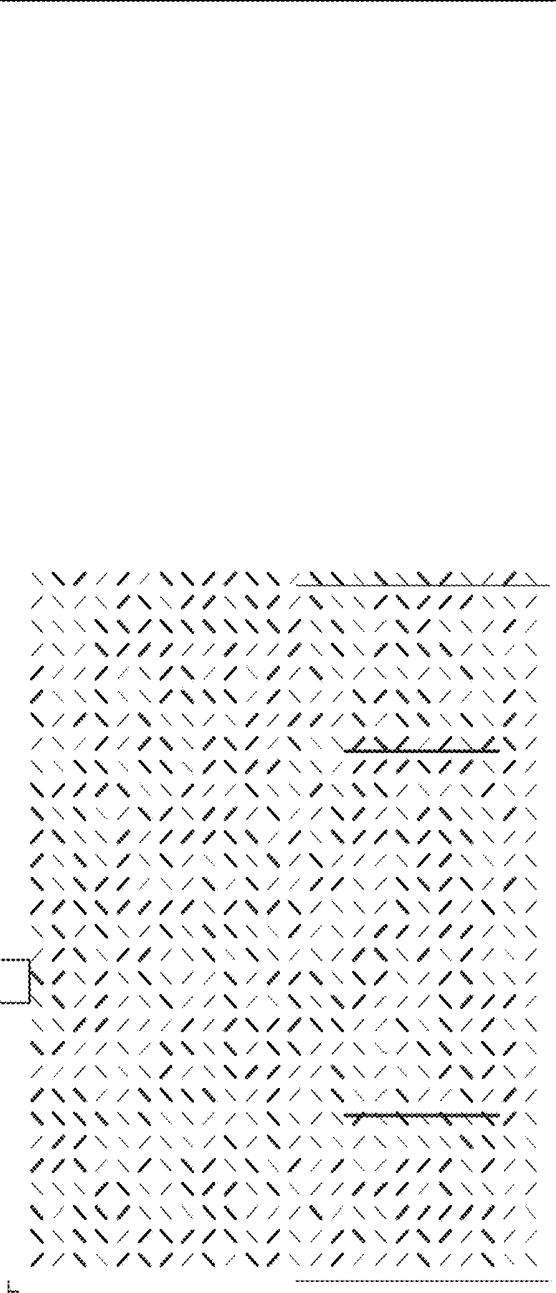
???	Access to file...	???	???	???	???	???	???	???	???	???
										
Time: 06-04-2018 18:57										
From: 1GQHPrvLi35hEy1K3B1dyf75WyzFHkFQ1v										
To: 7QPHrvLo55tEy1T3C6dyf22WrzPHInEL5x										
Amount: USD 1,000										
PIN: 83620248										

FIG.4

*QR code decrypted by the user 1*

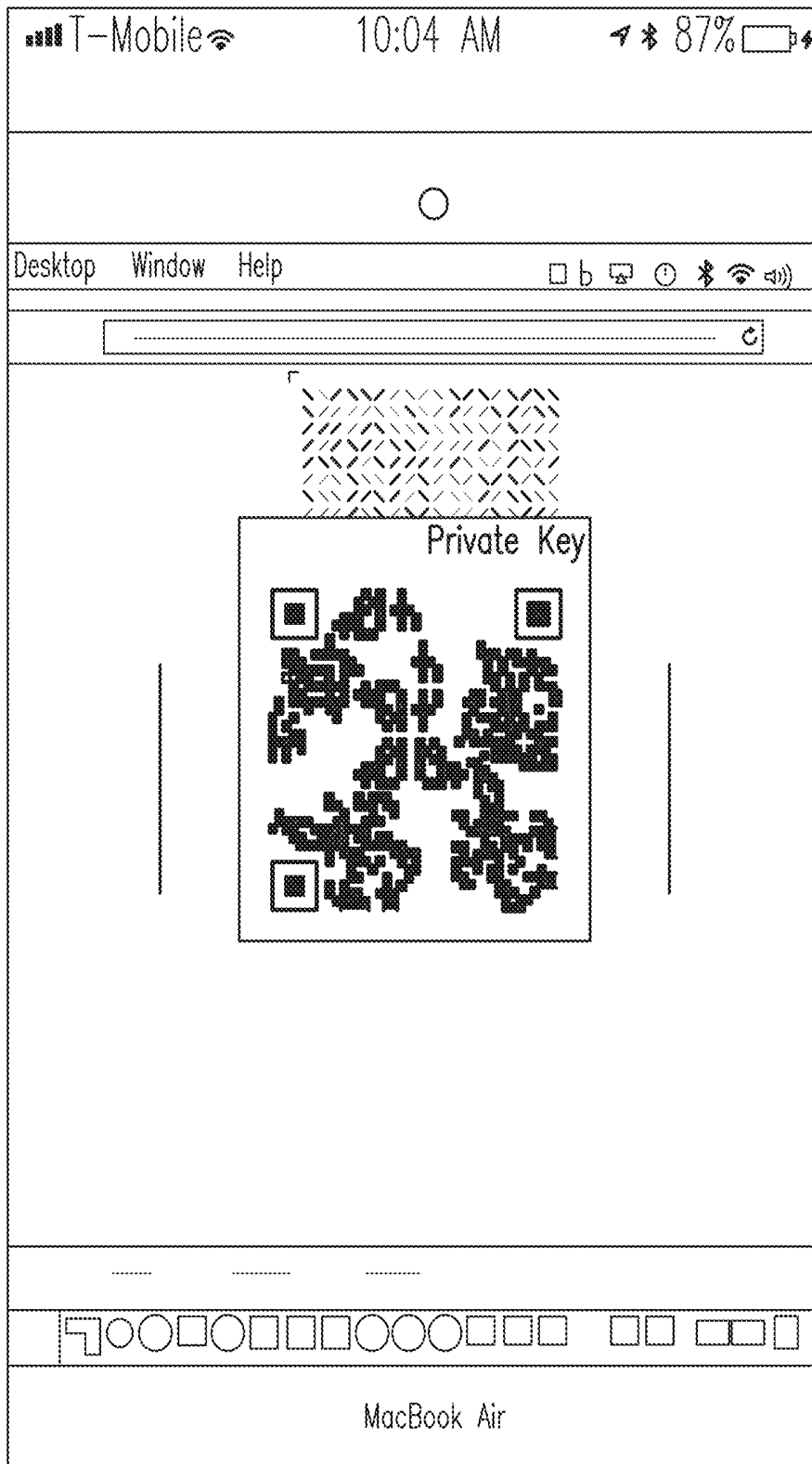


FIG.5

*Example of CAPTCHA replacement*

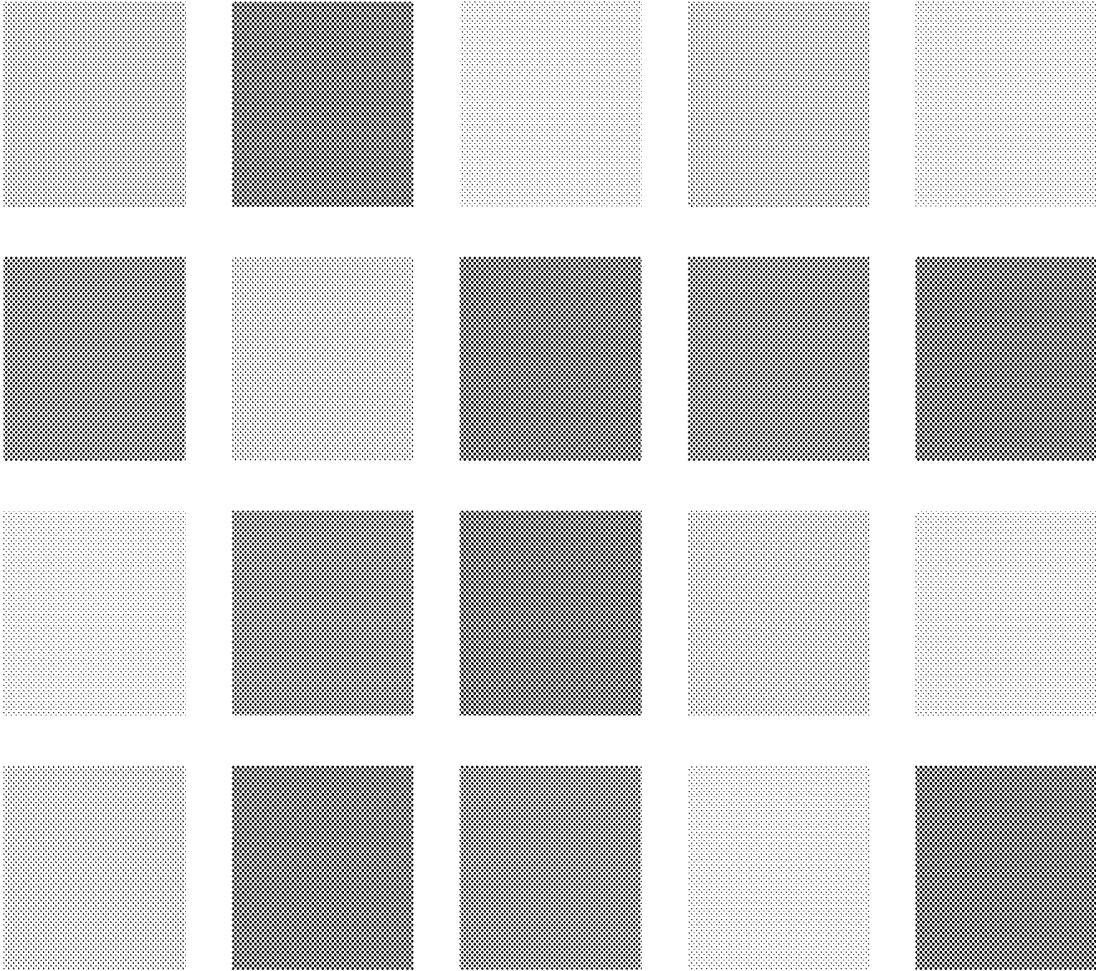


FIG.6

*Example of multi-party decryption*

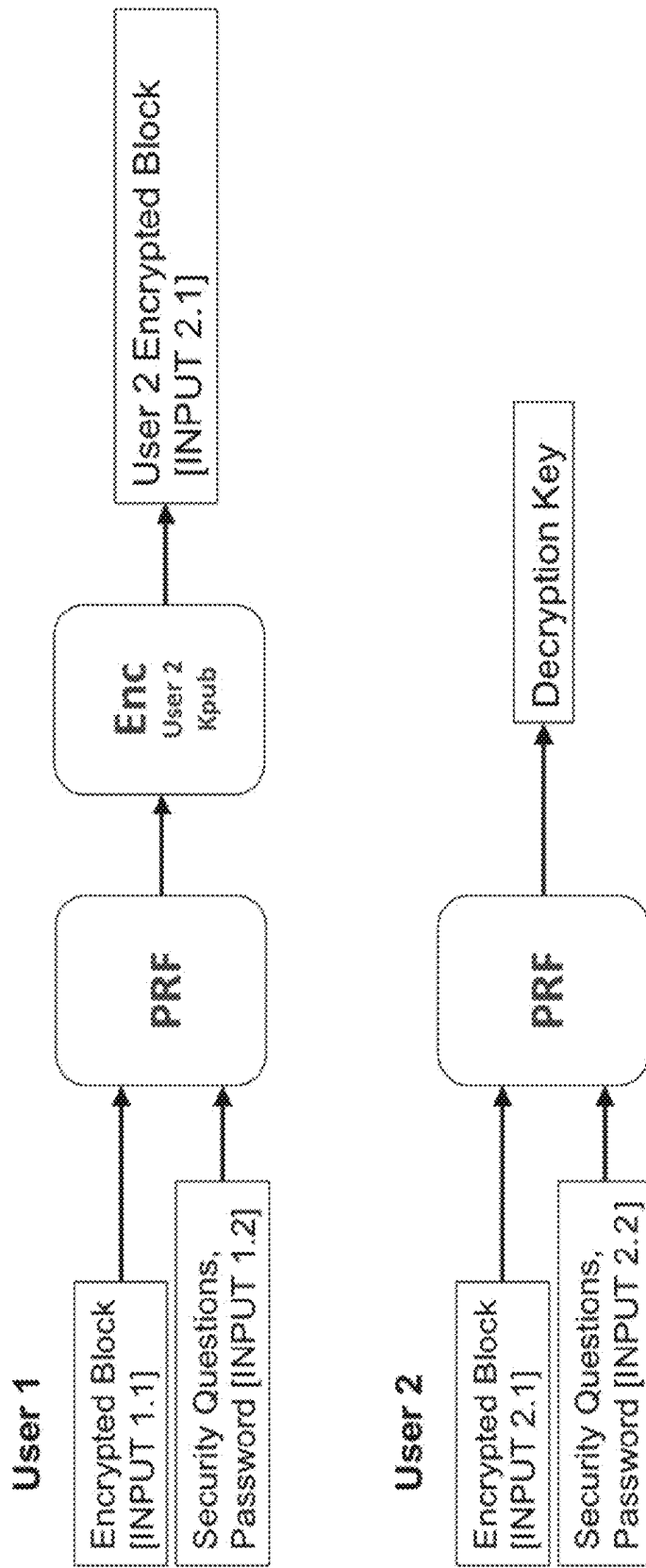


FIG. 7

Example of Verification Service With Two Approvals

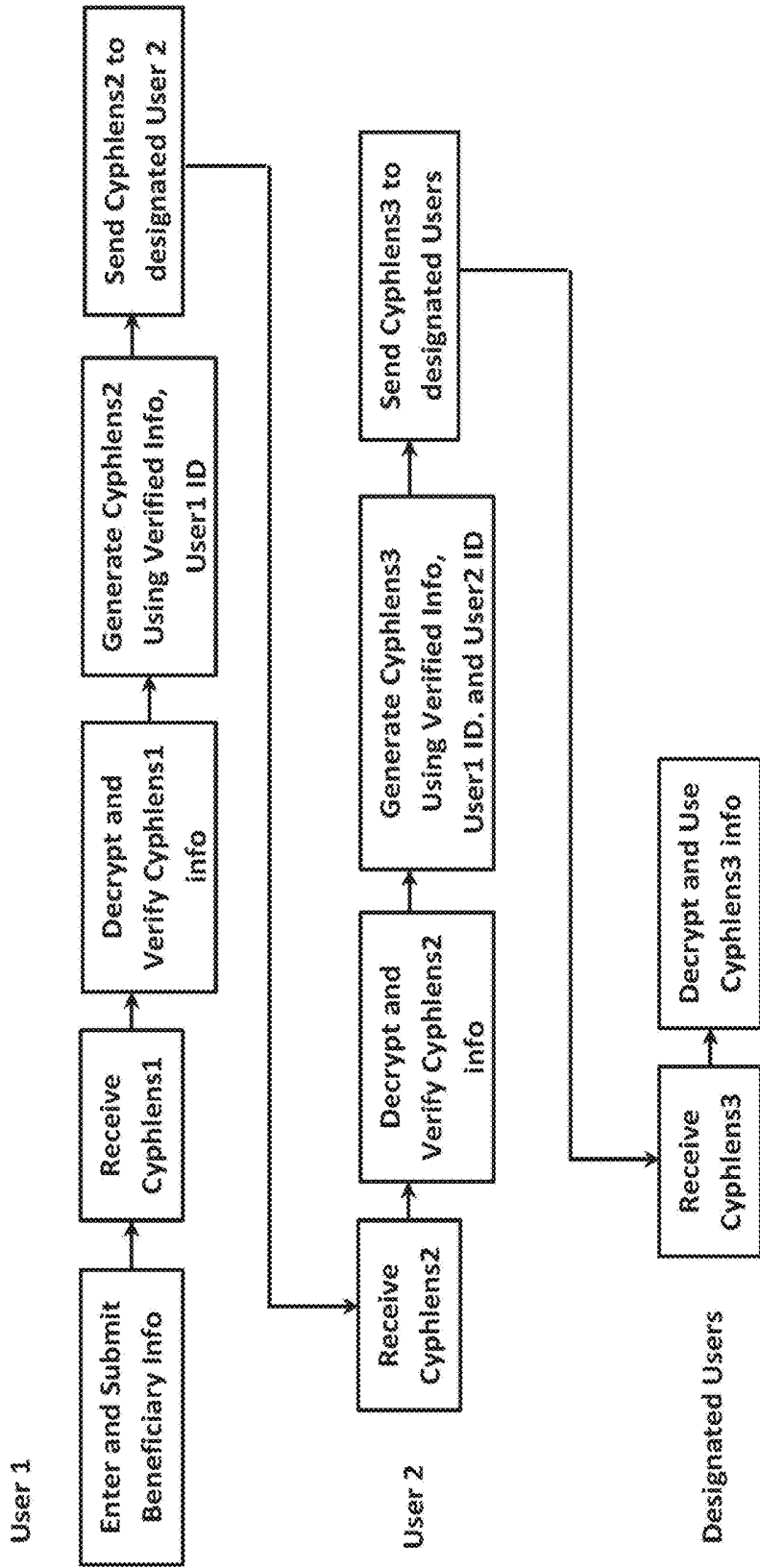


FIG. 8

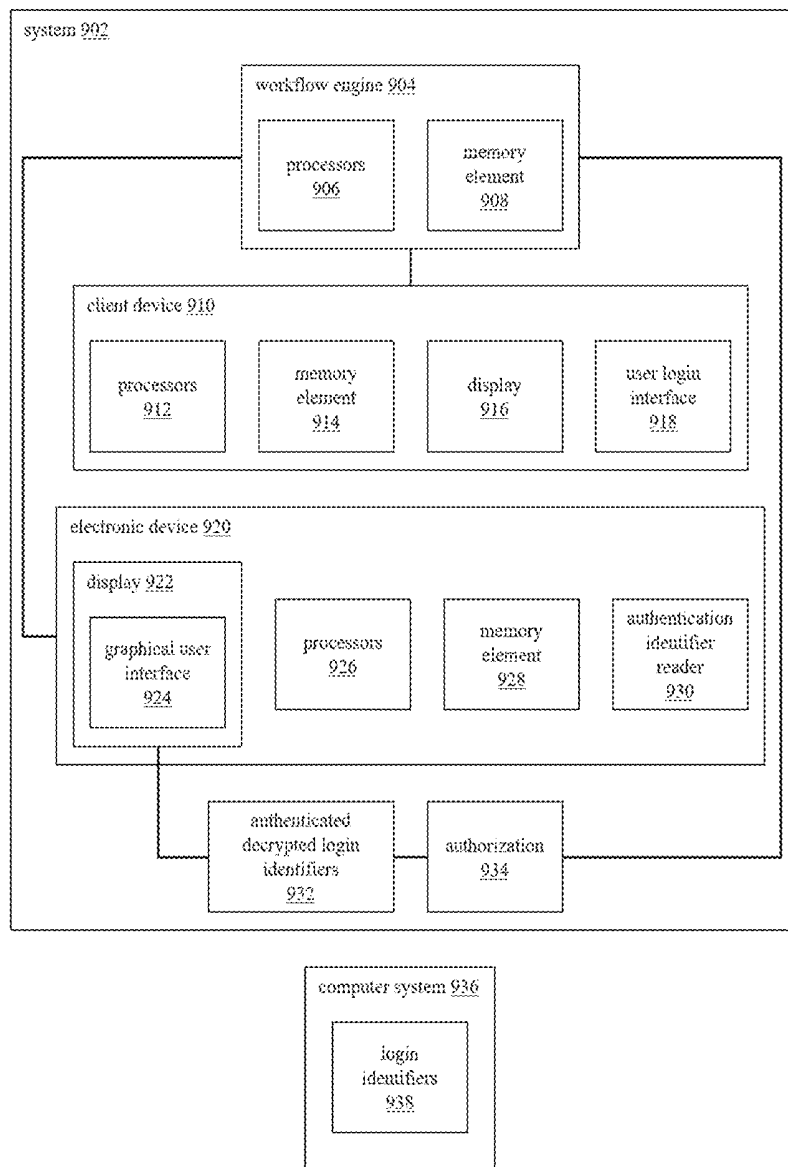


FIG. 9

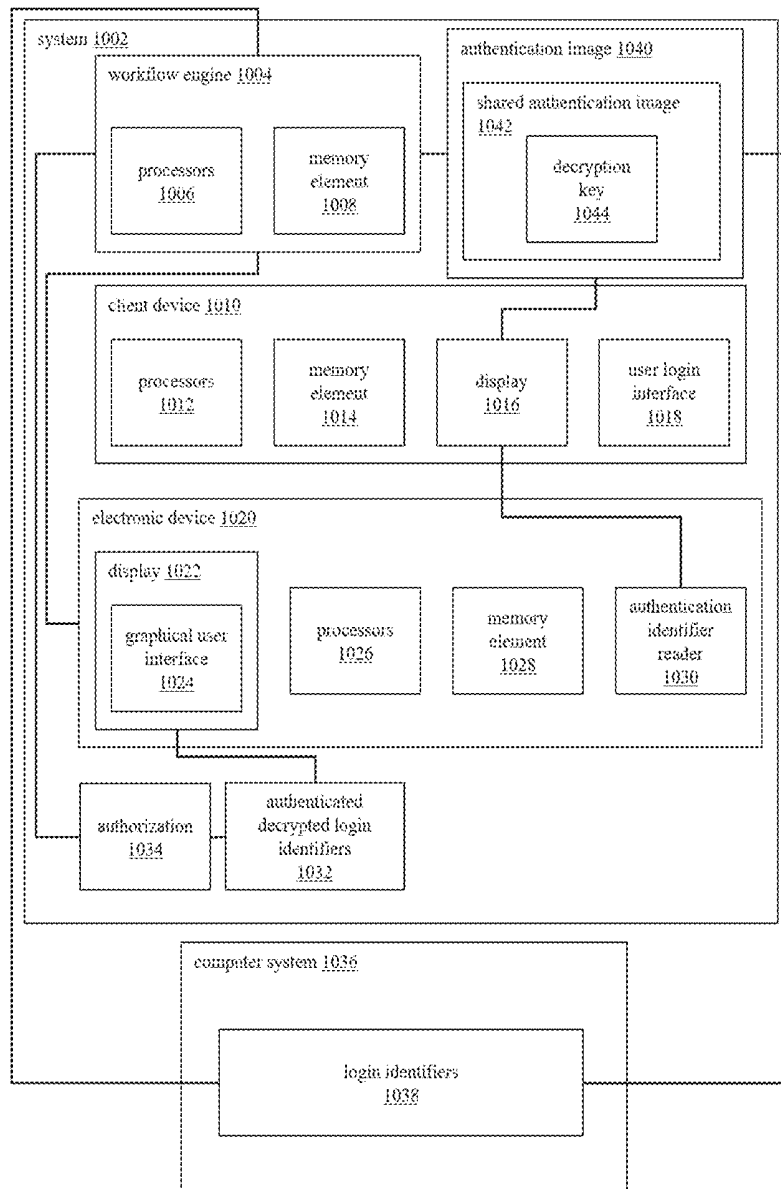
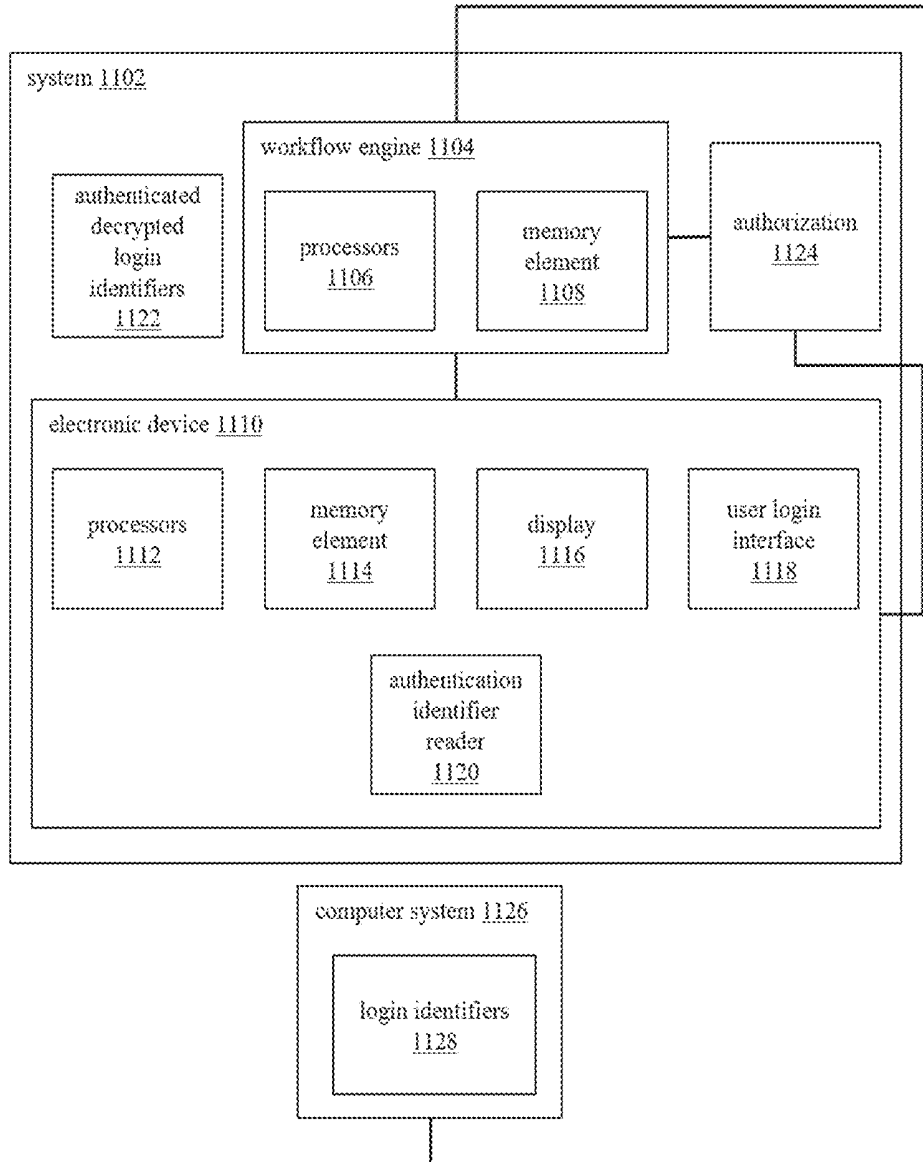
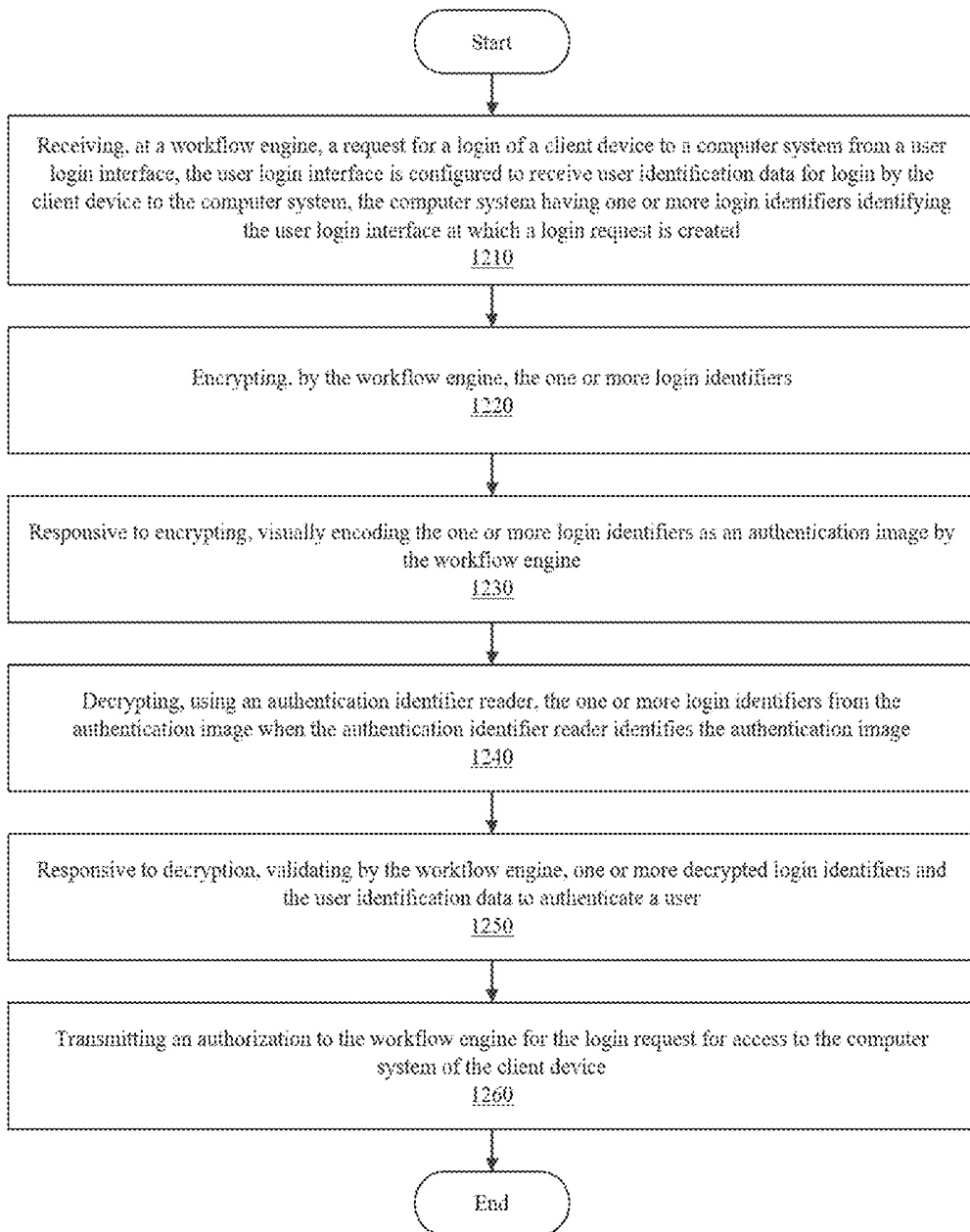
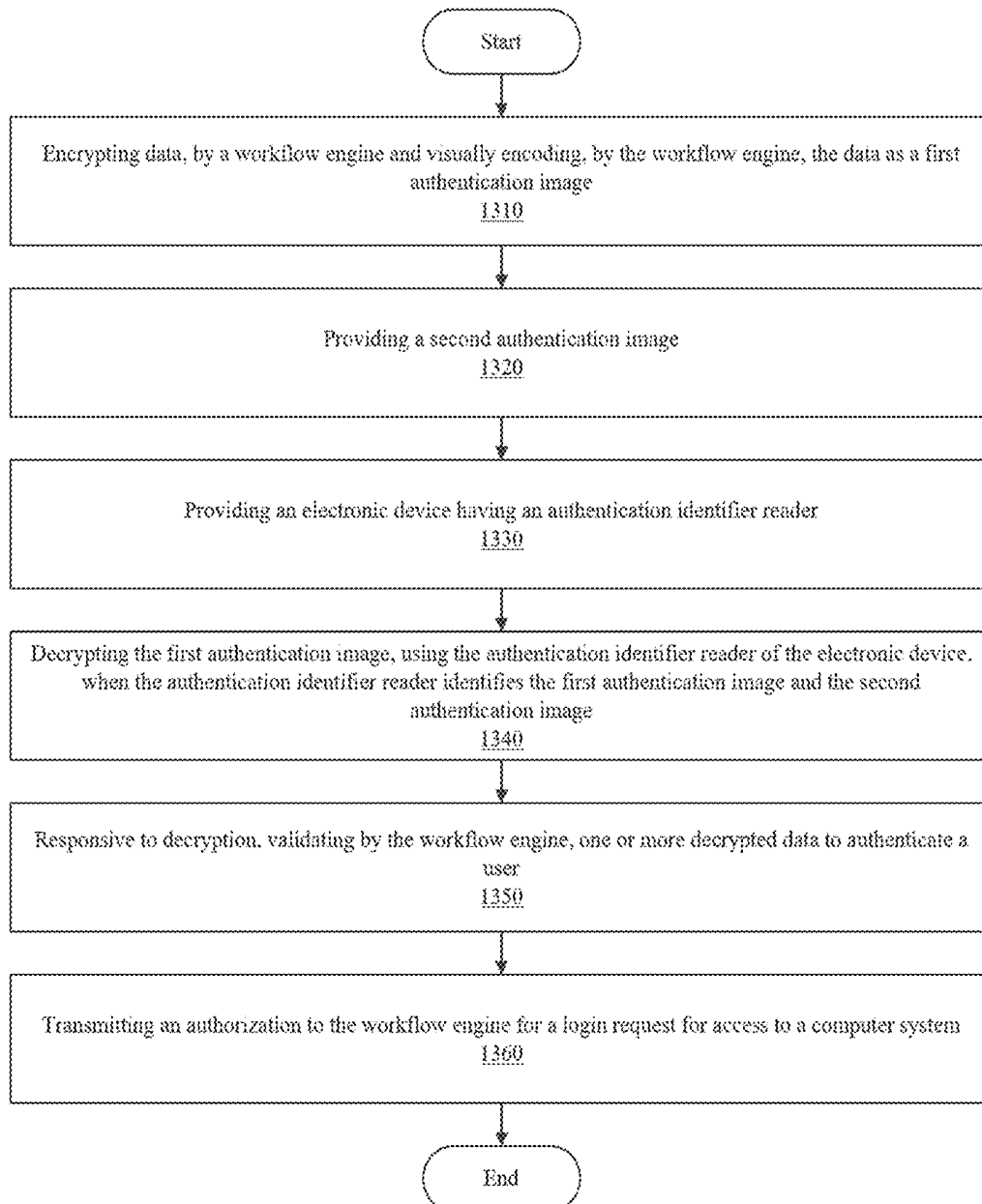


FIG. 10



**FIG. 11**

**FIG. 12**

**FIG. 13**

**CONTENT ENCRYPTION AND IN-PLACE  
DECRYPTION USING VISUALLY ENCODED  
CIPHERTEXT**

CROSS-REFERENCE TO RELATED  
APPLICATIONS

This application is a U.S. Continuation-In-Part patent application, which claims priority to currently pending U.S. Non-Provisional patent application Ser. No. 17/715,055, filed on Apr. 7, 2022, which issued as U.S. Pat. No. 11,676,515 on Jun. 13, 2023 and Continuation-In-Part patent application Ser. No. 18/140,626, filed on Apr. 28, 2023 which claims priority to U.S. Non-Provisional patent application Ser. No. 16/272,117 filed on Feb. 11, 2019 and issued as U.S. Pat. No. 11,335,214, the contents of all of which are hereby incorporated by reference in their entireties.

FIELD

This invention relates to content encryption and decryption using visually encoded ciphertext, and in particular to systems and methods for bidirectional two-factor remote user authentication.

BACKGROUND

Previous approaches to remote user authentication have typically relied on single-factor authentication methods, such as passwords or PINs, which are vulnerable to security breaches. These methods often lack the necessary level of security to protect sensitive information and are susceptible to unauthorized access. Additionally, these approaches do not provide a comprehensive solution for bidirectional authentication, where both the user and the computer system authenticate each other.

Some existing systems have attempted to address the limitations of single-factor authentication by implementing two-factor authentication methods. These methods typically involve the use of a secondary authentication factor, such as a physical token or a one-time password, in addition to a password or PIN. While these approaches provide an additional layer of security, they still do not fully address the need for bidirectional authentication and may require additional hardware or software components.

Other approaches have focused on remote user authentication through web-based terminals. These systems allow users to access computer systems remotely through a web interface. However, these approaches often rely on traditional single-factor authentication methods, such as passwords, and do not provide a comprehensive solution for bidirectional authentication.

However, none of these approaches have provided a comprehensive solution that combines the features described in this disclosure. The present invention aims to overcome the limitations of previous approaches by providing a system for bidirectional two-factor remote user authentication that utilizes one or more encrypted login identifiers and an authentication image for secure authentication between the user and the computer system. For example many network information systems assign a login function that may be used to establish a login to retrieve data from a service provider. Currently, the process of logging into many online systems such as some user interfaces of websites, applications, and/or performing some critical action, often requires a user input of a password. The password is often referred to as a first factor of authentication. However, in

today's market, with a greater increase in cyberattacks, the scientific community has introduced many other factors of authentication. Multi-factor authentication is an example of a security system requiring at least two different types of identification for the authorization of a login request. Some factors of identification are known as something you know, something you have, or something you are.

Something you know is a password. Something you are is a user biometrics (e.g., your fingerprint). Something you have is what many refer to as a second factor of authentication ("2FA") and may include, a text with a code, an email with a code, a phone call with a code or a physical token. Any combination of the three can be used in order to login into a website or perform a critical action (e.g., send money online). In particular, 2FA is a method where a user needs to provide an additional piece of data that proves ownership of the second factor (something you have). This second factor could be a hardware token or a cellphone, for example. In such a case, the hardware token or the cellphone would display a unique numeric code that the user needs to provide to the website in order to prove to the website ownership of the hardware token or cellphone (something you have).

In many of the typical 2FA solutions, the user further authenticates with the server by proving ownership of the second factor. However, the server does not authenticate with the user. In other words, this second factor authentication is a one-way authentication: the user further proves its identity to the server, but the server does not prove its identity to the user. Hence the plethora of phishing attacks where a server that has not been authenticated by the user requests sensitive information from the user (e.g., the user password). To address these problems, another authentication step may be implemented while avoiding a complex user login process. Thus, there is a need for an improved second factor authentication that authenticates the server to prove the server identity to the user. As a result, security may be enhanced

In many scenarios, only certain parts of a document contain sensitive information and need to be encrypted (e.g., account balance in a bank statement, SSN in a tax return). However, the present approach to encryption is "all or nothing", requiring an entire document to either be encrypted or not. A system and method for efficiently enabling users to selectively encrypt and visually embed pieces of data in a larger body of data is thus needed.

Examples of related art are described below:

U.S. Pat. No. 9,183,677 generally describes a system that allows a camera enabled application, such as an augmented reality application, to run in a protected area may include a first device including a camera, the camera including a secure mode of operation and a display, an image processing module configured to convert image data from the camera to encoded data when the camera is in the secure mode and protect image data stored in the system, an encryption module configured to encrypt encoded data from the image processing module, and a protected audiovisual path mechanism configured to securely send augmented encoded data to the display.

U.S. Pat. No. 9,213,854 generally describes a head-mounted display (HMD) apparatus and a method for accessing encrypted information by the apparatus, in which the head-mounted display apparatus with enhanced security includes a biometric information input unit that receives biometric information of a user; a communication module that transmits or receives information to or from a server; a memory that stores encrypted information; a processor that transmits the biometric information received through the

biometric information input unit to a user authentication server through the communication module, receives access privilege information from the user authentication server, and decrypts the encrypted information stored in the memory based on the received access privilege information; and a display unit that displays the decrypted information through the processor.

U.S. Pat. No. 9,251,366 generally describes a method, non-transitory computer readable medium and apparatus for decrypting a document are disclosed. For example, the method captures a tag on an encrypted document, transmits the tag to an application server of a communication network to request a per-document decryption key, receives the per-document decryption key if the tag is authenticated, and decrypts a portion of the encrypted document using a temporary decryption key contained in the tag, the tag decrypted with the per-document decryption key.

U.S. Pat. No. 9,330,272 generally describes a head-mounted display (HMD) apparatus and a method for accessing encrypted information by the apparatus, in which the head-mounted display apparatus with enhanced security includes a biometric information input unit that receives biometric information of a user; a communication module that transmits or receives information to or from a server; a memory that stores encrypted information; a processor that transmits the biometric information received through the biometric information input unit to a user authentication server through the communication module, receives access privilege information from the user authentication server, and decrypts the encrypted information stored in the memory based on the received access privilege information; and a display unit that displays the decrypted information through the processor.

U.S. Pat. No. 9,893,890 generally describes a method of decrypting an encrypted message. The method comprises storing a wearer decryption code in a memory of a wearable mobile device having a head-worn augmented display which generates an augmented reality view for a wearer of the wearable mobile device, capturing using the wearable mobile device a video sequence including at least one frame imaging a visible code using an image sensor of the wearable mobile device, processing the video sequence to identify the visible code, decrypting the visible code using the wearer decryption code to create an decrypted content, and presenting the decrypted content on top of at least some of the visible code in the augmented reality view.

U.S. Pat. No. 9,948,659 generally describes a system that allows a camera enabled application, such as an augmented reality application, to run in a protected area may include a first device including a camera, the camera including a secure mode of operation and a display, an image processing module configured to convert image data from the camera to encoded data when the camera is in the secure mode and protect image data stored in the system, an encryption module configured to encrypt encoded data from the image processing module, and a protected audiovisual path mechanism configured to securely send augmented encoded data to the display.

U.S. Patent Publication No. 2015/0295715 generally describes a method of decrypting an encrypted message. The method comprises storing a wearer decryption code in a memory of a wearable mobile device having a head-worn augmented display which generates an augmented reality view for a wearer of the wearable mobile device, capturing using the wearable mobile device a video sequence including at least one frame imaging a visible code using an image sensor of the wearable mobile device, processing the video

sequence to identify the visible code, decrypting the visible code using the wearer decryption code to create an decrypted content, and presenting the decrypted content on top of at least some of the visible code in the augmented reality view.

U.S. Patent Publication No. 2018/0167215 generally describes a method of decrypting an encrypted message. The method comprises storing a wearer decryption code in a memory of a wearable mobile device having a head-worn augmented display which generates an augmented reality view for a wearer of the wearable mobile device, capturing using the wearable mobile device a video sequence including at least one frame imaging a visible code using an image sensor of the wearable mobile device, processing the video sequence to identify the visible code, decrypting the visible code using the wearer decryption code to create an decrypted content, and presenting the decrypted content on top of at least some of the visible code in the augmented reality view.

International Patent Publication No. WO2014/005736A1 generally describes a method for providing private information to a user, comprising the steps of a) Encrypting one or more private messages including private information for one or more users, b) Encoding the encrypted one or more messages into a public content stream including public content for public presentation, c) Analog presenting of the public content stream, wherein the encoded one or more messages are human-unperceivable. d) Capturing the presented public content stream by a user device of a user, e) Decoding the one or more encrypted private messages from the captured public content stream for the user, f) Decrypting the decoded one or more encrypted private messages, g) Providing the decrypted private information to the user. It also relates to a system for providing private information to a user.

None of the art described above addresses all of the issues that the present invention does.

#### SUMMARY

A system for bidirectional two-factor remote user authentication includes a workflow engine comprising one or more processors and at least one memory element for storing instructions. The workflow engine generates and encrypts data such as, a plurality of website specific data including, but not limited to, one or more login identifiers. The system also includes a client device in communication with the workflow engine over a network. The client device comprises one or more processors, at least one memory element for storing instructions, a display, and a user login interface. The user login interface receives user identification data for login to a computer system. The workflow engine generates and encrypts one or more login identifiers, visually encoding them as an authentication image displayed on the client device's display. An electronic device, also in communication with the workflow engine, includes a display with a graphical user interface, one or more processors, at least one memory element storing the login identifiers and user identification data, and an authentication identifier reader. The reader decrypts the login identifiers from the authentication image, and upon decryption, the workflow engine validates the decrypted login identifiers and user identification data to authenticate the user. Authenticated login identifiers are displayed on the electronic device's display, and the user transmits authorization for the login request to the workflow engine for access to the computer system and which also includes improvements that overcome the limitations of

prior art two-factor authentication systems and methods are now met by a new, useful, and non-obvious invention.

An image is displayed to a user through a graphic user interface of a web-based terminal of a display of a client device. The image is scanned by a user's electronic device. Image processing on the image including decryption and key management according to the workflow engine. It is within the scope of this invention for the workflow engine to determine who has access to an image and how key distribution is allocated for the image after the image has been scanned by an electronic device of a user. In particular, transport layer security (TLS) key exchange allows two parties to use a cryptographic algorithm by exchanging cryptographic keys. In an example, a symmetric key is generated during a TLS handshake before an encrypted message is transmitted. Public Key Infrastructure (PKI) is an example over which symmetric keys are exchanged. In a PKI system, the client generates a public-private key pair. The public key and/or data intended to be embedded in the certificate are sent to a Certificate Authority (CA). The CA then creates a digital certificate consisting of the user's public key and certificate attributes. The certificate is signed by the CA with its private key. Symmetric Key Cryptography also known as Symmetric Encryption is when the same cryptographic key is leveraged for both encryption of the plaintext and decryption of the ciphertext. This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt. During this process, data is converted to a format that cannot be read or inspected by anyone who does not have the cryptographic key that was used to encrypt it. Both users, including the web-based terminal and the electronic device are required to both have access to the cryptographic key to maintain the private data pairing.

According to another aspect of the present invention, a method for encrypting and decrypting data using visually encoded ciphertext is provided. The method includes selecting, using a graphical user interface coupled to an electronic device, one or more portions of a document to be encrypted, visually encoding the selected one or more portions of the document, generating a visual representation, wherein the visual representation corresponds to encrypted content, and replacing the selected one or more portions of the document with the visual representation. The method further includes displaying, to the user, the visual representation, capturing the visual representation using one or more cameras, decoding the visual representation, obtaining the encrypted content, and decrypting the encrypted content, generating decrypted content.

In some aspects, the techniques described herein relate to a method for securely sharing data using visually encoded ciphertext, the method including: entering and submitting digital content by a first user (user1); receiving by user1 a visually encoded ciphertext (cyphlens1) containing an encryption of the digital content; decrypting the cyphlens1 image to verify the digital content encrypted therein; approving by user1 the cyphlens1 image containing the verified encrypted digital content for further use; encrypting the approved digital content in a second visually encoded ciphertext (cyphlens2), wherein: the cyphlens2 image can be decrypted only by a specified second user (user2); and the cyphlens2 image includes an identifier of user1; sending the cyphlens2 image to user2; receiving by user2 the cyphlens2 image; decrypting the cyphlens2 image by user2 to verify the information encrypted therein; approving by user2 the cyphlens2 image containing the verified encrypted information for further use; encrypting the digital content approved

by both user1 and user2 in a third visually encoded ciphertext (cyphlens3), wherein: the cyphlens3 image may be decrypted only by user1, user2, and other designated users; the cyphlens3 image includes the identifier of user1; sending the cyphlens3 image to the designated users; receiving by the designated users the cyphlens3 image; decrypting the cyphlens3 image by one or more of the designated users to respectively obtain the information encrypted therein.

In some aspects, the techniques described herein relate to a method, wherein at least one of user1 and user2 enters and submits information to be encrypted via one of a web form, an app, and an API (Application Programming Interface).

In some aspects, the techniques described herein relate to a method, wherein the cyphlens3 image further includes an identifier of user2.

In some aspects, the techniques described herein relate to a method, wherein at least one of user1 and user2 approves cyphlens1 and cyphlens2, respectively, by a respective at least one of an action using a touch screen, an action using a real or virtual keyboard, and an action using a biometric reader.

In some aspects, the techniques described herein relate to a method, wherein the decrypting of at least one of cyphlens1, cyphlens2, and cyphlens3 is accomplished using a mobile device with a camera.

In some aspects, the techniques described herein relate to a method, wherein the at least one of the cyphlens2 image and the cyphlens3 image is one of, a modified cyphlens1 image and a first newly generated image, and a modified cyphlens2 image and a second newly generated image, respectively.

In some aspects, the techniques described herein relate to a method, wherein at least one of the cyphlens2 image and the cyphlens3 image expires after a respective one of a select time or duration and a predetermined default time or duration.

In some aspects, the techniques described herein relate to a method, wherein the identifier of at least one of user1 and user2 is a respective email address or phone number.

In some aspects, the techniques described herein relate to a method, wherein at least one of the cyphlens2 image and the cyphlens3 image is sent via at least one of an email, a text message, a messaging app, a website, printed paper, a wired communication system, and a wireless communication system.

In some aspects, the techniques described herein relate to a method, wherein the cyphlens3 image is decrypted by at least one of user1 and user2.

In some aspects, the techniques described herein relate to a method, wherein one or more of the recipients of the cyphlens3 image further process at least one of the cyphlens3 image and the information decrypted therefrom.

In some aspects, the techniques described herein relate to a system for securely sharing data using visually encoded ciphertext, the system including a first graphical user interface, a first memory, and a first processor configured to: receive digital content submitted by a first user (user1); generate a visually encoded ciphertext (cyphlens1) containing an encryption of the submitted digital content; return the cyphlens1 to user1; responsive to a request received from user1, decrypt the cyphlens1 image for verification by user1 of the digital content encrypted therein; receive the verified digital content; generate a second visually encoded ciphertext (cyphlens2) containing an encryption of the verified digital content, wherein: the cyphlens2 image can be

decrypted only by a specified second user (user2); and the cyphlens2 image includes an identifier of user1; and send the cyphlens2 image to user2.

In some aspects, the techniques described herein relate to a system, further including: a second electronic device including a second graphical user interface, a second memory, and a second processor configured to: receive the cyphlens2 image; responsive to a request received from user2, decrypt the cyphlens2 image for verification by user2 of the information encrypted therein; receive the verified input data submitted by user2; generate a third visually encrypted image (cyphlens3) containing an encryption of the input data verified by user2, wherein: the cyphlens3 image can be decrypted only by user1, user2, and at least one other designated user (user3); the cyphlens3 image includes the identifier of user1; and the cyphlens3 image can be approved for further use only by ones of the at least one user3, and send the cyphlens3 image to the at least one user3.

In some aspects, the techniques described herein relate to a system, further including: at least one third electronic device including a third graphical user interface, a third memory, and a third processor configured to: receive the cyphlens3 image; responsive to a respective request received from a respective one or more of the at least one user3, decrypt the cyphlens3 image and provide to the respective user3 the information encrypted therein.

In some aspects, the techniques described herein relate to a system, wherein at least one of user1 and user2 enters and submits information to be encrypted via one of a web form, an app, and an API (Application Programming Interface).

In some aspects, the techniques described herein relate to a system, wherein the cyphlens3 image further includes an identifier of user2.

In some aspects, the techniques described herein relate to a system, wherein at least one of user1 and user2 approves cyphlens1 and cyphlens2, respectively, by a respective at least one of an action using a touch screen, an action using a real or virtual keyboard, and an action using a biometric reader.

In some aspects, the techniques described herein relate to a system, wherein the decrypting of at least one of cyphlens1, cyphlens2, and cyphlens3 is accomplished using a mobile device with a camera.

In some aspects, the techniques described herein relate to a system, wherein the at least one of the cyphlens2 image and the cyphlens3 image is one of, a modified cyphlens1 image and a first newly generated image, and a modified cyphlens2 image and a second newly generated image, respectively.

In some aspects, the techniques described herein relate to a system, wherein at least one of the cyphlens2 image and the cyphlens3 image expires after a respective one of a select time or duration and a predetermined default time or duration.

In some aspects, the techniques described herein relate to a system, wherein the identifier of at least one of user1 and user2 is a respective email address or phone number.

In some aspects, the techniques described herein relate to a system, wherein at least one of the cyphlens2 image and the cyphlens3 image is sent via at least one of an email, a text message, a messaging app, a website, printed paper, a wired communication system, and a wireless communication system.

In some aspects, the techniques described herein relate to a system, wherein the cyphlens3 image is further decrypted by at least one of user1 and user2.

In some aspects, the techniques described herein relate to a system, wherein one of the recipients of the cyphlens3 image further process at least one of the cyphlens3 image and the information decrypted therefrom.

In some aspects, the techniques described herein relate to a system for bidirectional two-factor remote user authentication, including: a workflow engine including: one or more processors; and at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors, the at least one memory element retains login data; a client device, the client device is in communication with the workflow engine over a network, the client device, including: one or more processors; at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors; a display; and a user login interface, the user login interface is configured to receive user identification data for login by the client device to a computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created, the one or more login identifiers are generated and encrypted by the workflow engine, wherein responsive to encryption, one or more encrypted login identifiers are visually encoded as an authentication image, the authentication image is displayed on the display of the client device; an electronic device, the electronic device is in communication with the workflow engine over the network, the electronic device, including: a display having a graphical user interface; one or more processors; at least one memory element, the at least one memory element stores the one or more login identifiers of the computer system and the user identification data; and an authentication identifier reader, the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image, wherein responsive to decryption, one or more decrypted login identifiers and the user identification data are configured to be validated, by the workflow engine, to authenticate a user, and wherein one or more authenticated decrypted login identifiers are configured to be displayed on the display of the electronic device, and an authorization for the login request for access to the computer system of the client device is configured to be transmitted, by the electronic device, to the workflow engine.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image within a predetermined distance from a predetermined location.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image at a predetermined time.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the one or more encrypted login identifiers having encrypted content.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image is a visual representation of the one or more encrypted login identifiers.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the electronic device having a camera, the camera is configured to capture the authentication image of the display of the client device.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image of the display of the client device is uploaded to the electronic device.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the user identification data is at least one of a username, an email address, or a password.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the electronic device having an input sensor disposed on the display of the electronic device, the input sensor sensing an external input to submit the authorization for the login request to the workflow engine.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authorization for the login request is transmitted to the workflow engine when the one or more authenticated decrypted login identifiers are input manually, by a user, into the computer system of the client device.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the computer system of the client device is configured to prompt a user to input the user identification data into the computer system of the client device.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, further including a symmetric key is generated during a pairing, using transport layer security, before the authentication image is imported into the electronic device.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, further including public key infrastructure encryption of the one or more login identifiers and decryption of the one or more login identifiers from the authentication image.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image is linked to a specific browser session.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image is valid for a configurable duration, the authentication image and the user identification data is invalidated after the configurable duration has been exceeded.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image is configured to be transmitted to the electronic device at time, the authentication image is configured to be decrypted at time with  $>$ .

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image is configured to be decrypted when decryption is performed within a predetermined range of a predetermined location.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the authentication image having geographical data.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication,

wherein the authentication image includes a shared authentication image having a decryption key.

In some aspects, the techniques described herein relate to a system for bidirectional two-factor remote user authentication, including: a workflow engine including: one or more processors; and at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors, the at least one memory element retains login data; an electronic device, the electronic device is in communication with the workflow engine over a network, the electronic device, including: one or more processors; at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors; a display; and a user login interface, the user login interface is configured to receive user identification data for login by the electronic device to a computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created, the at least one memory element is configured to store the one or more login identifiers of the computer system and the user identification data, the one or more login identifiers are generated and encrypted by the workflow engine, wherein responsive to encryption, one or more encrypted login identifiers are visually encoded as an authentication image, the authentication image is displayed on the display of the electronic device; and an authentication identifier reader, the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image, wherein responsive to decryption, one or more decrypted login identifiers and the user identification data are configured to be validated, by the workflow engine, to authenticate a user, and wherein one or more authenticated decrypted login identifiers are configured to be displayed on the display of the electronic device, and an authorization for the login request for access to the computer system of the electronic device is configured to be transmitted, by the electronic device, to the workflow engine.

In some aspects, the techniques described herein relate to a method for mutual two-factor remote user authentication, including: receiving, at a workflow engine, a request for a login of a client device to a computer system from a user login interface, the user login interface is configured to receive user identification data for login by the client device to the computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created; responsive to the request from the client device, the workflow engine generating one or more login identifiers; encrypting, by the workflow engine, the one or more login identifiers; responsive to encrypting, visually encoding the one or more login identifiers as an authentication image by the workflow engine; decrypting, using an authentication identifier reader, the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image; responsive to decryption, validating by the workflow engine, one or more decrypted login identifiers and the user identification data to authenticate a user; and transmitting an authorization to the workflow engine for the login request for access to the computer system of the client device.

In some aspects, the techniques described herein relate to a method, further including prompting a user, responsive to transmitting the authorization, to input the user identification data into the computer system of the client device to complete the login.

In some aspects, the techniques described herein relate to a method, further including transmitting the authentication image from the workflow engine to the client device and displaying the authentication image from a display of the client device.

In some aspects, the techniques described herein relate to a method, wherein the client device having the authentication identifier reader and responsive to decryption, the client device displaying one or more authenticated decrypted login identifiers on the display of the client device.

In some aspects, the techniques described herein relate to a method, wherein transmitting the authorization for the login request to the workflow engine when the one or more authenticated decrypted login identifiers are input manually, by a user, into the computer system of the client device.

In some aspects, the techniques described herein relate to a method, further including transmitting the authentication image from the workflow engine to an electronic device and displaying the authentication image from a display of the electronic device.

In some aspects, the techniques described herein relate to a method, wherein the electronic device having the authentication identifier reader and responsive to decryption, the electronic device displaying one or more authenticated decrypted login identifiers on the display of the electronic device.

In some aspects, the techniques described herein relate to a method, wherein transmitting the authorization for the login request to the workflow engine when the one or more authenticated decrypted login identifiers are input manually, by a user, into the computer system of the electronic device.

In some aspects, the techniques described herein relate to a method for mutual two-factor remote user authentication, including: encrypting data, by a workflow engine and visually encoding, by the workflow engine, the data as a first authentication image; providing a second authentication image; providing an electronic device having an authentication identifier reader; decrypting the first authentication image, using the authentication identifier reader of the electronic device, when the authentication identifier reader identifies the first authentication image and the second authentication image; responsive to decryption, validating by the workflow engine, one or more decrypted data to authenticate a user; and transmitting an authorization to the workflow engine for a login request for access to a computer system.

In some aspects, the techniques described herein relate to a method, wherein authorizing decryption, by a decrypting key of the electronic device.

In some aspects, the techniques described herein relate to a method, wherein encrypting the second authentication image with the data used for decrypting the first authentication image for a double second-factor authentication.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation is a still image.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation is part of a video feed.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein capturing the visual representation includes capturing two or more visual representations,

and wherein decoding the visual representation includes simultaneously decoding the two of more visual representations.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein decrypting the encrypted content further includes decrypting the encrypted content using predetermined cryptographic key material.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation includes one or more formats selected from the group consisting of: Quick Response Codes; data matrices; data glyphs, and/or any other relevant formats.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the method further includes displaying some or all of the decrypted content.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein displaying the encrypted content further includes overlaying the decrypted content over one or more objects.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the decrypted content is internally used by a computer system to perform one or more tasks.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the document includes a plurality of visual representations, and wherein the method further includes performing an integrity check of the encrypted content of the plurality of visual representations.

It is an object of the present invention to provide the method for encrypting and decrypting data using visually encoded ciphertext, wherein the performing the integrity check further includes generating a hash of each of the visual representations in an order in which each of the visual representations appears in the document and comparing the hash to a hash generated when the encrypted content was encrypted.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation is a still image.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation is part of a video feed.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein capturing the visual representation includes capturing two or more visual representations, and wherein decoding the visual representation includes simultaneously decoding the two of more visual representations.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein decrypting the encrypted content further includes decrypting the encrypted content using predetermined cryptographic key material.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the visual representation includes one or more formats selected from the group

consisting of: Quick Response Codes; data matrices; data glyphs, and/or any other relevant formats.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the second electronic device further includes a display, configured to display some or all of the decrypted content.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the decrypted content is internally used by a computer system to perform one or more tasks.

It is an object of the present invention to provide the system for encrypting and decrypting data using visually encoded ciphertext, wherein the document includes a plurality of visual representations, and wherein the second processor is further configured to perform an integrity check of the encrypted content of the plurality of visual representations.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a high-level pipeline used to convert data to visually encoded ciphertext, according to an embodiment of the present invention.

FIGS. 2A-2B show non-overlaid content (FIG. 2A) and overlaid content (FIG. 2B), according to an embodiment of the present invention.

FIG. 3 shows structure of encrypted content, according to an embodiment of the present invention.

FIG. 4 shows an example of transaction summary with PIN, according to an embodiment of the present invention.

FIG. 5 shows a QR code decrypted by a user, according to an embodiment of the present invention.

FIG. 6 shows an example of CAPTCHA replacement, according to an embodiment of the present invention.

FIG. 7 shows an example of multi-party decryption, according to an embodiment of the present invention.

FIG. 8 shows an example of a verification service with two approvals, according to an embodiment of the present invention.

FIG. 9 is a block diagram illustrating a system, according to some embodiments of the present disclosure.

FIG. 10 is a block diagram further illustrating the system from FIG. 9, according to some embodiments of the present disclosure.

FIG. 11 is a block diagram illustrating a system, according to some embodiments of the present disclosure.

FIG. 12 is a flowchart illustrating a method, according to some embodiments of the present disclosure.

FIG. 13 is a flowchart illustrating a method, according to some embodiments of the present disclosure.

#### DETAILED DESCRIPTION

Example embodiments of the present invention will now be described with reference to the drawings. Identical elements in the various figures are identified with the same reference numerals. These embodiments are provided by way of explanation of the present invention, which is not intended to be limited thereto. In fact, those of ordinary skill in the art may appreciate upon reading the present specification and viewing the present drawings that various modifications and variations can be made thereto.

A system is provided for encrypting and displaying private content in a public setting. In embodiments, this is done

by leveraging state of the art encryption, image processing and, optionally, an augmented reality user experience.

In embodiments, the present system enables the encryption of pieces of sensitive information (e.g., text, images, video) in a visual way. These pieces of sensitive information may be standalone or can be part of a larger document. Most documents do not require to be entirely encrypted, as only some parts in them are sensitive. With the present invention, users may choose to encrypt only those parts of a document that they deem sensitive and encrypt them in a visual way such that decryption is similar to a “point and shoot” user experience. In embodiments, the encrypted pieces are embedded into the document and placed in the exact same position of their non-encrypted counterparts. In embodiments, users need just to point their device’s camera to the encrypted pieces of information for decryption to take place on the fly, in real time. This new technology enables a plethora of new applications and provides novel solutions to a number of cyber-security attacks (e.g., phishing attacks, man-in-the-middle attacks).

In embodiments, the system includes one or more electronic devices. The electronic devices may include one or more cameras which may be configured to include Internet connectivity via a wired and/or wireless connection. In embodiments, the one or more electronic devices include a desktop computer, a laptop computer, a tablet computer, a smart phone, smart glasses, and/or any other suitable electronic device. In embodiments, the one or more electronic devices include one or more displays.

In embodiments, the present system encrypts and visually encodes content in such a way that, in order to decrypt the content, a user needs to use a device equipped with a display and one or more cameras. In embodiments, the visual representation of the encrypted content is captured by one or more image capture devices, either as a still image or as part of a video feed, and is decoded and decrypted.

In embodiments, the decrypted content may or may not be displayed to the user, depending on the specific scenario. In embodiments, if the content is displayed to the user, it may be overlaid over some other content (e.g., images, logo, ads, etc.) and “anchored” to it. This option of content overlayment over some other content provides users with an augmented-reality user experience. According to an alternate embodiment, the decrypted content may be displayed anywhere on the screen of the device (e.g., at the bottom of the screen).

If the device camera captures multiple visual encodings at once (either adjacent or not), the system can simultaneously decode and decrypt the content. If the decrypted data is meant for human consumption, the system can simultaneously display the content as an overlay over some other content or anywhere else on the screen of the device.

In embodiments, in order for the device to be able to decrypt content, the user device needs to have access to correct cryptographic key material. In embodiments, the system supports both symmetric-key encryption and asymmetric-key encryption.

In embodiments, content is provided by a user. Content provided by the user is encrypted and “formatted” in such a way that a visual representation of this encrypted content is created (an encrypted content image). In embodiments, this encrypted content image may be in the form of one or more QR codes, data matrices, data glyphs, and/or some other suitable visual representation, while maintaining the spirit of the present invention. In embodiments, a mix of multiple visual representations may be used for the same encrypted code (e.g., a QR code surrounded by data glyphs). In

embodiments, the user may select which content to be encrypted using a graphical user interface coupled to an electronic device. The electronic device may be, e.g., a desktop computer, a laptop computer, tablet computer, a smartphone, and/or any other suitable electronic device. In 5  
embodiments, there may be one or more electronic devices. The electronic devices may include at least a processor, a memory, a graphical user interface, a display, one or more cameras, and other relevant components.

In embodiments, encrypted content encoded in the 10  
encrypted content image may be of two different types: actual content and/or “pointers” to the actual content.

In embodiments, the actual content that either a user or a machine has provided and needs to consume is encrypted and visually encoded (the “actual content”). In embodi- 15  
ments, one or more pointers to the content to be consumed are encrypted and visually encoded (the “pointer”). A pointer, for example, could be a Uniform Resource Identifier (URI), an alphanumeric identifier (ID), and/or some other representation redirecting to the actual content. In embodi- 20  
ments, other metadata may also be present as part of the encrypted data. Content to be encrypted may be user-provided as well as machine-generated, and may be in a human-readable format or not.

In embodiments, in order to encrypt content, a plurality of 25  
operations are performed, the number of which depending on the functionality and user experience desired. For example, a flowchart showing high-level pipeline used to convert data to a visually encoded ciphertext is shown in FIG. 1.

According to various embodiments of the present inven- 30  
tion, decrypted content may be “anchored” to a specific location on a device screen, may be displayed anywhere on the device screen, and/or may not be displayed at all to a user and used internally.

In embodiments, if the decrypted content is anchored to a 35  
specific location on the device screen, the following may happen:

1. Encrypted content is decrypted from the corresponding 40  
encrypted code;
2. By using various image processing techniques, the encrypted code is erased from the augmented reality view. In embodiments, logos, images, ads and/or any other suitable visual objects may be placed in its place;
3. Decrypted information is put in place of the encrypted 45  
code or overlaid over (all or part of) the logo, image, ad and/or any other suitable visual objects that replaced the encrypted code.

An example of overlaid content over a commercial logo “anchored” to the location previously occupied by the 50  
encrypted code is illustratively depicted in FIG. 2B, in accordance with an embodiment of the present invention. The non-overlaid content is shown in FIG. 2A.

In embodiments, an operations pipeline may include the following: plaintext.fwdarw.encrypted.fwdarw.error 55  
correction.fwdarw.visual encoding. In such a scenario, compression may or may not be used.

In embodiments, with non-overlaid content, the plaintext is not anchored to a specific location or overlaid over other 60  
content, but may be displayed anywhere on the device screen.

The operations pipeline used in such a scenario may include the following: plaintext.fwdarw.compression.fwdarw.encrypted.fwdarw.error correction.fwdarw.visual encod- 65  
ing. In embodiments, compression can be applied since the size of the visual encoding does not need to match the size of the decrypted content, thus it can be smaller.

In the scenario of internally-used content, the ciphertext is decrypted and the corresponding plaintext is not displayed to the user, but it is used “internally” by the system. The operations pipeline used in such a scenario may be the same as in the previous case of non-overlaid content. For example, where such a situation may occur may include the digital signing of Blockchain transactions where the encrypted information is the wallet private key.

In embodiments, a mixed scenario may also occur where, 10  
given one encrypted code, some decrypted elements are displayed to the user and some other elements are used internally (e.g., metadata).

In embodiments, one or more encryption keys may be used. Both asymmetric-key and symmetric-key encryption may be used, according to various embodiments. In particu- 15  
lar, both per-document keys and per-user keys may be used, according to various embodiments.

Per-document keys may be used if the document will be 20  
shared among multiple parties. In such a case, each new document will use a different encryption key.

Per-user keys may be used if the document will be kept private and not shared with other parties. In such a case, multiple documents may use the same encryption key.

In embodiments, multiple visual encodings (either adja- 25  
cent or nonadjacent) may be captured and processed all at once. This includes the scenario of having multiple visual encodings of mixed type (e.g., QR codes and data glyphs). In embodiments, if multiple visual encodings (i.e., blocks) 30  
are present, these are completely independent from one another and do not share any kind of information with one another, i.e., they are stand-alone entities.

In embodiments, in order to see the decrypted content, users position their device camera over an area containing 35  
the visual encoding(s) of the encrypted content. In embodiments, through the camera, the device captures the bits of ciphertext by applying various image-processing techniques to the visual encoding. The device then fetches the decryption key(s) for that ciphertext from the backend, if these 40  
were not already present on the user device. Ciphertext is then decrypted (i.e., plaintext) and is displayed to the user either as an overlay or on some other part of the screen of the device. If the plaintext is not meant for user-consumption, it is not displayed to the user but it is used internally by the system.

In embodiments, the visual representation is, for example, a representation of either an encrypted pointer (e.g., URI, URL) to the content or an ID that identifies some property of the visual representation (e.g., its position in the world, the name of its owner) or something else. In embodiments, additional metadata may be present.

In embodiments, the decrypted data is not the actual content the user needs to see but it is a pointer to it or some metadata. In embodiments, once the pointer to the actual content has been decrypted, the user device connects to servers in the backend and fetches the proper encrypted content by using the decrypted pointer and any additional information (e.g., time of day, GPS coordinates of user device). A URI may point to an (encrypted) image or a video, for example. On the other hand, an ID may point to some image or text that may change over time as that same ID may give different content if queried at different times.

In embodiments, the content fetched from the backend may be displayed as an overlay or anywhere (e.g., at the bottom) on the screen of the device. If the content is not meant for user-consumption, it is not displayed to the user but it is used internally by the system.

In embodiments, for the encrypted content to be correctly visually decoded (especially if a custom visual encoding with no landmarks is used), it needs to be organized in a specific way in order to improve efficiency of the decoding process. In particular, before visually encoding the encrypted content, it is organized into a specific structure. One possible structure is shown in FIG. 3.

Generally speaking, Header and Body may use different visual encodings so that, for example, a lower-capacity but more robust visual encoding may be used for the Header in order to make it more resilient to errors. Examples of different visual encodings are: a QR code for the Header and data glyphs for the Body, a one-bit-per-glyph encoding for the Header and two-bit-per-glyph encoding for the Body, a QR code for the Header and data matrices for the Body. In the simplest case, both Header and Body may use the same visual encoding.

Looking now at each field of the structure and its meaning, in the following calculations, it is assumed that the Header is a 12x12 matrix (one-bit-per-glyph visual encoding).

Truncated Hash: truncated first 24 bits of a hash function (e.g., SHA256, HMAC) computed over all other fields of the Header.

Version: this field is NOT encrypted and it represents the version number of the block structure (bits: 24-31).

Rows: this field is NOT encrypted and is 8-bit long. It represents the number of rows in the block including the Header, that is, we can have an encrypted content block with a max number of  $256-12=244$  rows. (This field may be removed or re-assigned in future versions of the block structure.)

Cols: this field is NOT encrypted and is 8-bit long. It represents the number of columns in the block including the Header, that is, we can have an encrypted content block with max number of  $256-12=244$  columns. (This field may be removed in future versions of the block structure.)

Control Bits: this field may contain some special bits (e.g., checksum for error correction, parity bytes, MAC, hash of other fields) and if so, the size of this field may change. Right now it contains either the truncated hash of the encrypted content or some error-correction bits.

Encrypted Content: this field is the actual encrypted content and is N-bit long where N is a variable number up to  $(244*244*2)$  bits as per Rows/Cols fields described above. This means a maximum of 14,884 ASCII characters of (encrypted) content into a single block. The size of the following optional field (i.e., M bits) has to be subtracted by these calculations if such a field is present.

Extra Data: this field is optional. If required by the encryption algorithm, additional data may be appended in the Body after the Encrypted Content field. This extra data would be used only for decryption operations and, as such, it would not be considered part of the encrypted content. Its size is variable. In embodiments, the encryption algorithm can be any state-of-the-art encryption algorithm such as AES256 in GCM mode.

Given the structure defined above, one possible way to search for a valid encrypted block using the present invention is herein described.

In embodiments, when the device searches for an encrypted block, it first performs various image-processing transformations (e.g., convert image to a gray-scale, apply Gaussian Blur and other filters). Once the initial image processing is complete, the device starts looking for the beginning of a block. In particular, it computes the hash of the 96+8+8+8 bit fields in the Header that it sees and it

compares the first 24 bits of this hash to the 24 bits of the Truncated Hash field. If the two match, the device has found a valid block. If the two do not match, the beginning of a valid block has not been found and the search needs to continue.

If a valid block has been found, we look at the Version field first in order to know what version of the block structure this is. In particular, the version number tells us how to interpret the various fields in the block and specific bits within a field. For example, for different versions we may use different header structures, different encryption algorithms or give different meanings to the Control Bits field. Similarly, different versions may define different boundaries, thus different sizes, of the various fields.

In version 0, the Control Bits field may contain the truncated hash of the encrypted content. In other versions, on the other hand, such a field may contain: a checksum, an error correction code, a truncated hash of the Encrypted Content field, a Message Authentication Code (MAC), or other. In the case of error correction, this should take place before attempting decryption. In the case of truncated hash of encrypted content, hash verification should take place before attempting decryption in order to make sure that the correct header has been read for the correct content.

After looking at the Version field, we look at the Rows/Cols fields so that we know how many bits we need to read in order to correctly decrypt the encrypted content. Once this is known, we can proceed to read the remaining bits and attempt decryption. In particular, in version 0, the encrypted content to decrypt may be given by the N bits.

Once the encrypted content has been correctly decrypted, it can be either displayed to the user or used "internally" by the system as described above.

In embodiments, multiple encrypted blocks may be scattered throughout a document. It is important to make sure that the order in which these blocks were originally inserted in the document has not been changed. Furthermore, it is important to make sure that none of the blocks have been replaced with some other block not meant to be in that document. In other words, we need to verify the integrity of the encrypted content.

In order to verify integrity, when the encrypted blocks are generated, a hash of all of them is computed. In particular, the headers of the encrypted blocks (or the full blocks) are collected in the exact order in which they appear in the document and a hash (e.g., SHA256) of all of them is computed and saved.

Before performing decryption, if a user wants to verify the integrity of the encrypted parts of a document, it captures the encrypted blocks in the order they appear so that the device can generate the hash. Such hash is then compared to the one generated at encryption time and if the two match then integrity verification succeeds otherwise it fails. A visual cue may be shown to the user in either case.

When capturing blocks for integrity verification, they can be captured all at once by the user or one by one. However, if they are captured in the wrong order, integrity verification will fail. Furthermore, if decryption of any of the blocks fails, integrity verification will also fail.

The technology described herein pertaining to the present invention may be used in a number of novel use cases. Some of which are herein described below. It is noted, however, that the present invention may be used in other novel use cases not mentioned, while maintaining the spirit of the present invention.

Verification Service: In this use case users can secure their online account on a given website so that even if it gets hacked (i.e., a malicious actor can login into the user account) they can:

1. Verify if a transaction/action they are submitting is indeed what they meant to submit/do and no malicious actor modified it in any way;
2. Make sure that no malicious actor can perform an unauthorized transaction/action from their account.

In order to do this, a summary of the transaction (including a transaction ID) is encrypted together with a random PIN/string in an encrypted code. For the transaction to be submitted, users decrypt the encrypted code as described in one of the previous sections and see a summary of the transaction together with a random PIN, for example. Users can see and verify the summary of the transaction to make sure that everything is in order and proceed by inserting the random PIN in an opposite field on the website. Once the PIN is verified, the transaction is executed.

If a malicious actor has modified a transaction initiated by the user the malicious actor would not have access to encryption keys therefore would not be able to generate a fake encrypted summary of such transaction. The modified transaction would then be shown to the user in the encrypted summary and the user would then be able to detect it and decide not to proceed. Similarly, if the malicious actor initiates a new unauthorized transaction, he or she would not be able to decrypt the summary and read the random PIN to use in order to proceed with the transaction. Furthermore, the user may get notified and alerted with the encrypted transaction summary so that he or she may take appropriate action. FIG. 4 shows an example of a Bitcoin transaction summary using the verification service.

Multi-party decryption: In a multi-party decryption, in order to decrypt or unlock some data, multiple parties are required to take part in the process. There are two ways this can be accomplished:

1. Multiple parties operate sequentially; and
2. Multiple parties operate in parallel.

Furthermore, when operating in parallel, external automata can act as the gatekeeper (e.g., a multi-signature contract in the Ethereum blockchain) where two instances (from either the same or different users) are required to have decrypted the same content and signed the transaction in order for the transaction to go through.

For both parallel and sequential modes of operation, the method may involve parts of the same key held by different parties or it might involve keys of encryption keys creating a chain of custody, or it might involve disparate information needed to create or retrieve the encryption/decryption keys.

Three examples of how multi-party decryption may work follow. In a first example, we encrypt some data and encode it in a QR code, for example. The whole QR code is then encrypted using a different encryption key. When decryption needs to happen, one party is given the decryption key to decrypt the QR code and another party is given the decryption key to decrypt the content of the QR code.

FIG. 5 shows the decryption of the QR code by the first user. Once decrypted, the device of the second user can scan the QR code and decrypt its content. Such a device, in fact, will have the decryption key to decrypt the content of the QR code.

It is important to notice that the QR code and its encryption can be built in such a way so that the same QR code cannot be used more than once. In doing so, we prevent a situation where the second user takes a picture of the QR code (i.e., after user 1 has decrypted it) and uses it anytime

he or she wants without requiring the first user to be there. In order for this to be possible, the encryption of the QR code may be a URL pointing to a dynamically created encrypted QR code.

FIG. 7 illustrates a second example, in which User 1 has access to an encrypted block containing some input data (INPUT1.1) and User 2 has access to an encrypted block containing a wallet private key or some sensitive data to decrypt. In such a scenario, User 1 decrypts an encrypted block containing an input value (INPUT1.1). He or she then inserts answers to security questions, a password or similar (INPUT 1.2). Both inputs INPUT1.1+INPUT1.2 are then used as inputs to a PRF or similar function. User 1 then encrypts the output of the PRF [INPUT 2.1] using User 2 public key and encodes it in an encrypted block, a QR code or other visual encoding (this can be time limited, single use, etc.). User 2 decrypts this encrypted block using its private key and gets the input (INPUT 2.1). As a second step, User 2 inserts answers to security questions, a password or similar (INPUT 2.2). Both inputs INPUT 2.1+INPUT 2.2 are then used as inputs to a PRF or similar function. The output of the function is the encryption key that User2 needs to use in order to decrypt the encrypted block with the wallet private key or other sensitive data for User 2.

FIG. 8 illustrates a third example wherein, as part of the verification service, a flow may reflect a multi-step approval process. In the following, two approvals are described, but any number of approvals could be used, and the number of approvals is not a limitation. Further, although use of a "cyphlens image" (i.e., a visual encoding of encrypted content) is described, other forms of encoding could be used, and the encoding used is not a limitation. In addition in the following, although beneficiary information is described, any kind of digital content may be used. The content may also be in any of a variety of formats, such as text, images, video, or a combination of formats, that may be submitted, and may advantageously use or require the multi-step approval process described.

In this example usage case, User1 enters and submits beneficiary information, such as via a website, an app, or an API (Application Programming Interface). Here, the beneficiary is simply someone who derives an advantage from something. User1 receives back a visually encoded ciphertext ("cyphlens1") image containing the encrypted beneficiary information that they just submitted. User1 then decrypts the cyphlens1 image to obtain the beneficiary information encrypted therein using their mobile device or its camera or the like, and verifies it. If the beneficiary information obtained from the cyphlens1 image is correct (i.e., is not modified), User1 approves the cyphlens1 image for use, such as by performing an action using a touch screen, an action using a real or virtual keyboard, and/or an action using a biometric reader. For example, the approval may entail an action such as swiping, entering a password or PIN, or the like. Moreover, only User1 may approve the cyphlens1 image for further use.

Next, the beneficiary information approved by User1 is again encrypted in a new "cyphlens2" image, or a modified cyphlens1 image. The cyphlens2 image may be characterized by at least one of the following:

The cyphlens2 image may expire after a predetermined or selected time, or it may not expire at all.

Only a specified User2 can decrypt the cyphlens2 image. The cyphlens2 image includes the email address or other identifier of User1.

The cyphlens2 image is then sent to User2. The image may be sent via at least one of an email, a text message,

a messaging app, a website, printed paper, a wired communication system, and a wireless communication system.

User2 decrypts the cyphlens2 image to obtain the information encrypted therein using their mobile device or its camera or the like, and verifies it. If the decrypted information is correct, User2 approves the cyphlens2 image for use, such as by performing an action using a touch screen, an action using a real or virtual keyboard, and/or an action using a biometric reader.

Next, the beneficiary information that was approved by both User1 and User2 is again encrypted in a new cyphlens3 image, or in a modified cyphlens2 image. The cyphlens3 image may be characterized by at least one of the following:

The cyphlens3 image may expire after a predetermined or selected time, or it may not expire at all.

The cyphlens3 image may be decrypted only by User1, User2, and at least one other designated user (user3).

The cyphlens3 image may be approved only by at least one User3 for future use.

The cyphlens3 image includes the email address or other identifier of User1, and optionally the email address or other identifier of User2.

The cyphlens3 image (or modified cyphlens2 image) is sent to the designated users, such as via at least one of an email, a text message, a messaging app, a website, printed paper, a wired communication system, and a wireless communication system. The recipients of the new or modified cyphlens3 image may then decrypt the cyphlens3 image to obtain the information encrypted therein using their respective mobile devices, cameras, or the like. The recipients may then further process the cyphlens3 image and/or the information decrypted therefrom.

As described in the foregoing, user1 specifies the second user who will approve (user2) and user2 will specify the third user (user3). However in other embodiments, the identity of user2 may be unknown to user1; and the same may be true with regard to user2 and user3 and all other users. The list of users and their respective roles in this process may be configured by an admin who manages this process. The system may then make sure to forward the various encrypted cyphlens images to the correct users step by step.

Enforcing Multi-Party Access: Previously we have seen how it is desirable that, in multi-party decryption involving two users, User 2 can decrypt its encrypted content without User 1 taking action (e.g., User 2 could take a picture of the QR code decrypted by User 1 and use it at any time without User 1 even noticing). In the following we describe a possible way to enforce the presence of both User 1 and User 2 in order to decrypt content and prevent the aforementioned problem.

When a QR code is encrypted in an encryption block, some metadata can be associated with this QR code. Such metadata may include: number of times this QR code can be decrypted (see FIG. 5), a date after which decrypting of the QR code is disabled, time allowed to decrypt the content of the QR code from the moment the QR code was decrypted, and so on. In particular, the hash of the encryption block and the hash of the QR code are saved on the server with the associated metadata.

In one of many scenarios, when User 1 decrypts the QR code (see FIG. 5), the hash of the encrypted block is sent to the server and the event of the decryption will be registered with the server in the backend.

When User 2 scans the QR code (displayed by User 1) in order to decrypt its content, his or her device will send the hash of the QR code to the server. The server will check the metadata associated with the QR code and will grant or deny its decryption. For example, decryption of the content of the QR code may be possible only within a certain amount of time from the moment the QR code was decrypted by User 1. Similarly, decryption of the content of the QR code may be possible only a limited amount of times after which attempts to decrypt the content of the QR code would fail.

It is important to note that QR codes are just used as an example and that any other visual representation may be used in their place.

Ice-Cold Wallet Transactions: An ice-cold wallet is a cold wallet where Blockchain private keys are encrypted in an encryption code and printed on paper (i.e., kept offline). Furthermore, the decryption keys used to decrypt the Blockchain private keys are also encrypted in a different encryption code and printed on paper (i.e., kept offline).

Such "offline" content can be kept in bank vaults or any other location and can be decrypted by using a mobile application or any automaton following the protocol specified in the invention.

When the user needs to sign a transaction, he or she needs to decrypt the encryption code containing the Blockchain private keys. In order to do this the following happens:

1. The user device retrieves (from the company servers) the decryption keys used to decrypt the decryption keys of the wallet.
2. The user device decrypts the decryption keys and proceeds to decrypt the Blockchain private keys.
3. The user device loads the Blockchain private keys and signs the transaction on the device.
- 3a. Alternatively, the signing can be done on another server where the keys are made available securely
4. The signed transaction can be moved "online" into the Blockchain or sent to a blockchain node

In embodiments, when performing a multi-party transaction, there are two modes of operation for signing the transaction: parallel and sequential.

In parallel mode, user 1 signs the transaction and sends it to (company) servers. At the same time user 2 signs the same transaction and sends it to the company servers independently from user 1. The company servers, interacting with the Blockchain will post the transaction to the Blockchain (e.g., Ethereum) where it will be validated once signed by both users. This validation can be done using another smart contract or some in-memory logic.

In sequential mode, user 1 and user 2 need to sign the transaction one after the other before such a transaction is posted to the Blockchain. Once user 1 signs the transaction, he or she can send the partially signed transaction to user 2's device (e.g., via NFC, VPN) so that also user 2 can sign it. Only after both users sign the transaction, such a transaction is sent to the (company) servers that will then publish it to the Blockchain (e.g., Bitcoin).

Also, in this use-case, we can have both multi-party and single-party modes of operation.

Time-Based Decryption: At any time, in the previous use cases, the ability to decrypt an encrypted code can be revoked on demand by revoking the decryption key associated with that document. For time-based decryption, we enhance this functionality by allowing the content creator to specify an expiration deadline for an encrypted code. In doing so, whomever has access to such encrypted code, will be able to decrypt it up to the expiration deadline. Once the deadline has passed, decryption keys will be removed and/or

erased from all (or some) users' devices having access to this encryption code. Furthermore, additional steps may be taken in order to prevent users from decrypting the expired encryption code (e.g., decryption fails if the device has no Internet access).

**CAPTCHA Replacement:** In such use cases, we encrypt a pattern of squares, such as those shown in FIG. 6. In embodiments, the squares are colored squares. In embodiments, the user is then asked to press on the screen all the squares of a certain color (e.g., press all the yellow squares). Alternatively, we can ask users to follow more complex patterns such as alternatively pressing squares of two different colors (e.g., alternatively press yellow and red squares) until all squares of those two colors have been pressed. Other mechanisms not involving colors may also be used.

**Mutual Authentication:** Content may be encrypted by using either symmetric key encryption or asymmetric key encryption. When asymmetric keys are used the content may be additionally signed by the party encrypting it and the signature included in the encrypted content.

When encrypted content is decrypted by the user (and signature is verified in the case of asymmetric keys) the authentication of both parties can be implied.

In particular, assuming symmetric-key encryption, the encrypted content may include, among other things, a time-stamp of the encryption, an alphanumeric code, any other identifier of the other party. For a website, such identifier can be the domain name associated with the website, for example:

On the user side, by decrypting such encrypted content (and by verifying the signature if asymmetric-key encryption is used), the user can assume that the remote party is the legitimate party since it had the correct secret keys necessary to perform the encryption (or sign it). Additionally, the decrypted domain name, in the case of authentication to a website, can be visually verified by the user and compared to the domain name appearing in the browser address bar or similar.

On the other-party side (e.g., a webserver), the user is authenticated by providing the alphanumeric code provided as part of the encrypted content. This alphanumeric code can be a single-use code. By providing such code to the webserver, the user proves that has access to the crypto-material necessary to correctly decrypt such code and hence is the legitimate user.

This mutual authentication scheme can be used for various use-cases such as website login and multi-factor authentication. In particular, the user provides his or her username (or any other unique identifier) and the remote party (e.g., a website) replies with the encrypted content described above where content was encrypted using the crypto-material assigned to that user.

**Sharing Images:** Images can be shared by encrypting and encoding a URL to the image with some additional metadata. Such metadata may include, for example, a random alphanumeric code necessary in order to download and display the image to the user.

In particular, when a user decrypts the encrypted code pointing to an image, the user device will process the decrypted URL and will provide the decrypted alphanumeric code to the backend. Only if successful, the image will be downloaded and displayed to the user.

In embodiments, additional metadata may be included in the encrypted content or may be provided by the user device (e.g., time of day, location information). Such additional information may be used to enable new services (e.g.,

location based services) and provide different content to the user (e.g., a store coupon code) when paired with the encrypted/decrypted content.

For example, an encrypted code with an encrypted URL may be used to display an alphanumeric code to give access to a restricted area. Such a decrypted URL together with time of day and the device location would return an image of an alphanumeric code to use at that time for access to the restricted area. The user could then use such code in order to enter the restricted area. At a different time of day a different code may be displayed for the same encrypted content. Access to the decrypted image may be denied if the device location does not match the encrypted code location.

**Paper Documents:** Encrypted codes can be used to encrypt pieces of sensitive information in paper documents and the likes. Examples include: social security cards, passports, company ID cards, tax returns. Furthermore, additional data decryptable only by Government or company officials may be included in such documents.

For example, a passport may include an encrypted code containing personal information such as full name, date of birth, passport number, expiration date, picture of the passport owner. Such information may also be present in unencrypted text form. A government official may verify if a passport is counterfeit or not by comparing the text in the passport with the encrypted information in the encrypted code. Furthermore, there could be some other information encrypted on the passport, which may contain (or point to) sensitive content such as violations, police records, DMV records, decryptable only by the government/company official and not by the passport owner.

**Mixed Media:** A paper (or electronic) card containing an encryption block needs to be placed in the same camera view with other encryption blocks (either electronic or paper). By placing the blocks in the right order, an Integrity Verification operation is performed and if it succeeds then decryption happens by using as decryption key the key encrypted in the paper card encryption block.

In embodiments, in a different scenario, a password encrypted in the paper card is displayed to the user only if an Integrity Verification operation succeeds.

In embodiments, a multi/second factor device (i.e., hardware or software) may need to be updated under different circumstances. For example, the user may decide to upgrade their cell phone device or perhaps their cell phone gets stolen. In either of these cases, the user needs access to their digital assets in order to take some action.

According to one scenario, for example, if a user upgrades his or her cell phone device, an encrypted challenge is displayed to the user. This challenge can be decrypted with the old device and its content can be inserted (together with some other information such as username and password) in a form on the new device in order to trigger a new registration or login from the new device thus connecting old device/identity to new device. A second factor is then transferred to the new device.

According to another scenario, for example, in order to recover from the loss of a second factor device (software or hardware) without requiring a re-boarding or re-installation of a new second factor, the concept of human second factor recovery is introduced.

FIG. 9 is a block diagram that describes a system 902, according to some embodiments of the present disclosure. In some embodiments, the system 902 may include a workflow engine 904 and one or more authenticated decrypted login identifiers 932 may be configured to be displayed on the display 922 of the electronic device 920. The system 902

may also include a client device **910**, the client device **910** may be in communication with the workflow engine **904** over a network. The system **902** may also include an electronic device **920**, the electronic device **920** may be in communication with the workflow engine **904** over the network. The system **902** may also include an authorization **934** for the login request for access to the computer system **936** of the client device **910** that may be configured to be transmitted, by the electronic device **920**, to the workflow engine **904**.

In some embodiments, the workflow engine **904** may include one or more processors **906**. The workflow engine **904** may also include at least one memory element **908**, the at least one memory element **908** configured to store instructions for controlling the one or more processors **906**, the at least one memory element **908** retains login data. The client device **910** may include one or more processors **912** and a display **916**. The client device **910** may also include at least one memory element **914**, the at least one memory element **914** is configured to store instructions for controlling the one or more processors **912**. The client device **910** may also include a user login interface **918**, the user login interface **918** may be configured to receive user identification data for login by the client device **910** to a computer system **936**.

In some embodiments, the electronic device **920** may include a display **922** and one or more processors **926**. The electronic device **920** may also include at least one memory element **928**. The at least one memory element stores the one or more login identifiers **938** of the computer system **936** and the user identification data. The electronic device **920** may also include an authentication identifier reader **930**, the authentication identifier reader **930** may be configured to decrypt the one or more login identifiers **938** from the authentication image **1040** when the authentication identifier reader **930** identifies the authentication image **1040**.

In some embodiments, the display **922** may include a graphical user interface **924**. Responsive to decryption, one or more decrypted login identifiers and the user identification data may be configured to be validated, by the workflow engine **904**, to authenticate a user. The computer system **936** may also include one or more login identifiers **938** identifying the user login interface **918** at which a login request may be created, the one or more login identifiers **938** may be generated and encrypted by the workflow engine **904**. Responsive to encryption, one or more encrypted login identifiers may be visually encoded as an authentication image **1040**, the authentication image **1040** may be displayed on the display **916** of the client device **910**.

In some embodiments, the authentication identifier reader **930** may be configured to decrypt the one or more login identifiers **938** from the authentication image **1040** when the authentication identifier reader **930** may identify the authentication image **1040** within a predetermined distance from a predetermined location. In some embodiments, the authentication identifier reader **930** may be configured to decrypt the one or more login identifiers **938** from the authentication image **1040** when the authentication identifier reader **930** may identify the authentication image **1040** at a predetermined time.

In some embodiments, the one or more encrypted login identifiers may include encrypted content. In some embodiments, the authentication image **1040** may be a visual representation of the one or more encrypted login identifiers. In some embodiments, the electronic device **920** may also include a camera, the camera may be configured to capture the authentication image **1040** of the display **922** of the client device **910**.

In some embodiments, the authentication image **1040** of the display **922** of the client device **910** may be uploaded to the electronic device **920**. In some embodiments, the user identification data may be at least one of a username, an email address, or a password. In some embodiments, the electronic device **920** may also include an input sensor disposed on the display **922** of the electronic device **920**, the input sensor sensing an external input to submit the authorization **934** for the login request to the workflow engine **904**.

In some embodiments, the authorization **934** for the login request may be transmitted to the workflow engine **904** when the one or more authenticated decrypted login identifiers **932** may be input manually, by a user, into the computer system **936** of the client device **910**. In some embodiments, the computer system **936** of the client device **910** may be configured to prompt a user to input the user identification data into the computer system **936** of the client device **910**.

In some embodiments, the system **902** for the bidirectional two-factor remote user authentication. In some embodiments, the system **902** for the bidirectional two-factor remote user authentication. In some embodiments, the authentication image **1040** may be linked to a specific browser session. In some embodiments, the authentication image **1040** may be valid for a configurable duration, the authentication image **1040** and the user identification data may be invalidated after the configurable duration. Been exceeded.

In some embodiments, the authentication image **1040** may be configured to be transmitted to the electronic device **920** at time, the authentication image **1040** may be configured to be decrypted at time with  $>$ . In some embodiments, the authentication image **1040** may be configured to be decrypted when decryption may be performed within a predetermined range of a predetermined location. In some embodiments, the authentication image **1040** may include geographical data.

FIG. **10** is a block diagram that further describes the system **902** from FIG. **9**, according to some embodiments of the present disclosure. In some embodiments, the authentication image **1040** may include a shared authentication image **1042**. The shared authentication image **1042** may include a decryption key **1044**.

FIG. **11** is a block diagram that describes a system **1102**, according to some embodiments of the present disclosure. In some embodiments, the system **1102** may include a workflow engine **1104** and one or more authenticated decrypted login identifiers **1122** may be configured to be displayed on the display **1116** of the electronic device **1110**. The system **1102** may also include an electronic device **1110**, the electronic device **1110** may be in communication with the workflow engine **1104** over a network. The system **1102** may also include an authentication identifier reader **1120**, the authentication identifier reader **1120** may be configured to decrypt the one or more login identifiers **1128** from the authentication image when the authentication identifier reader **1120** identifies the authentication image. The system **1102** may also include an authorization **1124** for the login request for access to the computer system **1126** of the electronic device **1110** may be configured to be transmitted, by the electronic device **1110**, to the workflow engine **1104**.

In some embodiments, the workflow engine **1104** may include one or more processors **1106**. The workflow engine **1104** may also include at least one memory element **1108**, the at least one memory element **1108** configured to store instructions for controlling the one or more processors **1106**,

the at least one memory element **1108** retains login data. The electronic device **1110** may include one or more processors **1112** and a display **1116**. The electronic device **1110** may also include at least one memory element **1114**, the at least one memory element **1114** configured to store instructions for controlling the one or more processors **1112**. The electronic device **1110** may also include a user login interface **1118**, the user login interface **1118** may be configured to receive user identification data for login by the electronic device **1110** to a computer system **1126**.

In some embodiments, responsive to encryption, one or more encrypted login identifiers may be visually encoded as an authentication image, the authentication image may be displayed on the display **1116** of the electronic device **1110**. Responsive to decryption, one or more decrypted login identifiers and the user identification data may be configured to be validated, by the workflow engine **1104**, to authenticate a user. The computer system **1126** may also include one or more login identifiers **1128** identifying the user login interface **1118** at which a login request may be created, the at least one memory element **1114** may be configured to store the one or more login identifiers **1128** of the computer system **1126** and the user identification data, the one or more login identifiers **1128** may be generated and encrypted by the workflow engine **1104**.

FIG. **12** is a flowchart that describes a method, according to some embodiments of the present disclosure. In some embodiments, at **1210**, the method may include receiving, at a workflow engine, a request for a login of a client device to a computer system from a user login interface, the user login interface may be configured to receive user identification data for login by the client device to the computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request may be created.

In some embodiments, at **1220**, the method may include encrypting, by the workflow engine, the one or more login identifiers. At **1230**, the method may include, responsive to encrypting, visually encoding the one or more login identifiers as an authentication image by the workflow engine. At **1240**, the method may include decrypting, using an authentication identifier reader, the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image. At **1250**, the method may include, responsive to decryption, validating by the workflow engine, one or more decrypted login identifiers and the user identification data to authenticate a user. At **1260**, the method may include transmitting an authorization to the workflow engine for the login request for access to the computer system of the client device. Responsive to the request from the client device, the workflow engine generating one or more login identifiers.

In some embodiments, the method may include prompting a user, responsive to transmitting the authorization, to input the user identification data into the computer system of the client device to complete the login. In some embodiments, the method may include transmitting the authentication image from the workflow engine to the client device and displaying the authentication image from a display of the client device.

In some embodiments, the client device having the authentication identifier reader and responsive to decryption, the client device displaying one or more authenticated decrypted login identifiers on the display of the client device. In some embodiments, transmitting the authorization for the login request to the workflow engine when the one or

more authenticated decrypted login identifiers may be input manually, by a user, into the computer system of the client device.

In some embodiments, the method may include transmitting the authentication image from the workflow engine to an electronic device and displaying the authentication image from a display of the electronic device. In some embodiments, the electronic device having the authentication identifier reader and responsive to decryption, the electronic device displaying one or more authenticated decrypted login identifiers on the display of the electronic device. In some embodiments, transmitting the authorization for the login request to the workflow engine when the one or more authenticated decrypted login identifiers may be input manually, by a user, into the computer system of the electronic device.

FIG. **13** is a flowchart that describes a method, according to some embodiments of the present disclosure. In some embodiments, at **1310**, the method may include encrypting data, by a workflow engine and visually encoding, by the workflow engine, the data as a first authentication image. At **1320**, the method may include providing a second authentication image. At **1330**, the method may include providing an electronic device having an authentication identifier reader. At **1350**, the method may include, responsive to decryption, validating by the workflow engine, one or more decrypted data to authenticate a user. At **1360**, the method may include transmitting an authorization to the workflow engine for a login request for access to a computer system. At **1340**, the providing may include decrypting the first authentication image, using the authentication identifier reader of the electronic device, when the authentication identifier reader identifies the first authentication image and the second authentication image. In some embodiments, authorizing decryption, by a decrypting key of the electronic device. In some embodiments, encrypting the second authentication image with the data used for decrypting the first authentication image for a double second-factor authentication.

It is within the scope of this invention for an authentication image to include any visual representation, such as data matrices and/or Cyphlens images to name a few examples.

In a preferred embodiment, a plurality of login identifiers are stored in the at least one memory element. It is within the scope of this invention for an authorization to be determined by at least one authentication factor, one of which is by using one or more login identifiers in the system processing. For example a URL, an alphanumeric code, a logo image, a timestamp, a location, a one-time passcode and/or other data may be utilized by the system to determine authorization.

It is within the scope of this disclosure for user identification data to include, but not be limited to, a password, a username, and/or an email of a computer server to verify 2FA.

It is within the scope of this disclosure for communication, electrical communication, electrically coupled, and/or electrically connected to include, but not be limited to, a wired and/or a wireless connection.

It is within the scope of this disclosure for the workflow engine to be the backend server. The authentication image is displayed by the display of the client device. A client device may be any electronic device having access to a login interface to a computer system of a remote party including, but not limited to a website. The electronic device is the user mobile device, the client device, and/or a remote user device. The authentication image is read by the reader of the electronic device.

It is within the scope of the disclosure for an authorization to be determined by the workflow engine based on at least one authentication factor, one of which is by using one or more login identifiers in the system processing. For example, a URL, an alphanumeric code, a logo image, a timestamp, a location, a one-time passcode, and/or other data, and/or a combination may be utilized by the system to determine authorization.

It is within the scope of this invention for the method to include determining a presence of a match, by a user, if one or more decrypted login identifiers displayed on the electronic device matches the one or more login identifiers of the client device.

It is within the scope of this invention for one or more login identifiers to include, but not be limited to, any encrypted content, such as a uniform resource locator (URL), an alphanumeric code, a logo image, a timestamp, a location, a one-time passcode and/or other data and/or a combination of the aforementioned.

#### ADDITIONAL DESCRIPTION

It is within the scope of this invention for the system to include an improved second factor, hereinafter referred to as a mutual 2FA, a two-way 2FA, and/or a bidirectional two-way 2FA that works both ways or bidirectional in which the user proves ownership of the second factor thus further authenticating with the server and the server also provides further proof of its identity and therefore authenticates with the user.

Cyphlens technology, at its core, leverages encryption and decryption of data. Content may be encrypted by using either symmetric key encryption or asymmetric key encryption or a combination of both. When asymmetric keys are used the content may be additionally signed by the party encrypting it and the signature included in the encrypted content. When encrypted content is decrypted by the user (and the signature is verified in the case of asymmetric keys) the authentication of both parties can be implied. In particular, assuming symmetric-key encryption, the encrypted content may include, among other things, a timestamp of the encryption, a unique alphanumeric code and any other identifier of the encrypting party. For a website, for example, such an identifier can be the domain name associated with the website. When the 2FA authentication needs to take place, the following can happen: On the user side, by decrypting the System 2FA image encrypted content (and by verifying the signature if asymmetric-key encryption is used), the user can assume that the remote party is the legitimate party since it had the correct secret keys necessary to perform the encryption (and/or sign it). Additionally, the decrypted domain name, in the case of 2FA authentication to a website, can be visually verified by the user and compared to the domain name appearing in the browser address bar or similar (by employing image processing and other techniques this step may also be automated). On the other-party side (e.g., a web-server), the user is authenticated by providing the unique alphanumeric code provided as part of the encrypted content. This alphanumeric code can be a single-use code. By providing such a code to the web-server, the user proves that he has access to the crypto-material necessary to correctly decrypt such code (something you have) and hence is the legitimate user.

In other words, only the legitimate party (e.g., web-server) can encrypt (and/or sign) such content for the user and only the legitimate user can decrypt such content and provide the unique alphanumeric code as proof of correct

decryption. This mutual authentication scheme can be used for various use-cases such as a website login with two-factor authentication. In particular, for symmetric key encryption, the following may happen: the user provides his or her username (or any other unique identifier) to a remote party (e.g., a website) the remote party (e.g., a website) using the secret crypto material specific for that user encrypts some content using state of the art encryption primitives and algorithms. As mentioned above, the encrypted content may contain a unique alphanumeric code, a website URL, a logo image, a timestamp and other information related to either the website or the user or both.

The encrypted content is visually encoded in a QR code, a bar code, data matrices, a Cyphlens image, and/or any other visual representation. A combination of any of them is also possible. For the current example, assuming a Cyphlens image is used in this case. The Cyphlens image is then displayed on the website to the user. The user may use either their mobile device camera or by directly loading the Cyphlens image into their mobile device, decrypts the content using their specific secret crypto material. If decryption is successful (the user is the legitimate user), the decrypted information is displayed to the user on the mobile device and the user can verify its correctness (e.g., website URL, logo, and more). The unique alphanumeric code may also be shown to the user. If all the information looks correct, the user can use a gesture such as a swipe on the mobile device UI in order to submit the 2FA authentication to the web-server. As an alternative, the user can manually input the unique alphanumeric code into the website page and submit it from the website to the web-server.

In some aspects, the techniques described herein relate to a system for the bidirectional two-factor remote user authentication, wherein the graphical user interface of the display of the electronic device has an input sensor disposed on the display. The input sensor sensing an external input applied from the outside. The external input may include various types of inputs provided from the outside of the electronic device. The external input may be any one of various types of external inputs, such as a part of the user's body by a hand of the user and/or by a stylus as by way of example, embodiments are not limited thereto. As described above, the external input of the user may be provided in various types to activate the authorization for the login request with the client device to the computer system. For example, touch input of a user may include, but not be limited to, a press, a swipe, and/or a tap of the display of the electronic device as a controller means to indicate if a user wishes to proceed with the authorization process.

Once the 2FA step has completed successfully, the website prompts the user to input their password in order to complete the login process. Many variations of the sequence of events above are possible. The sequence described above where the user specifies the username, then completes the 2FA authentication and lastly inputs their password, has some advantages when using Cyphlens 2FA. In particular, because Cyphlens 2FA uses encrypted data that only the legitimate website can create, it disables all those phishing attacks that try to steal a user password. Typically, a phishing website would ask the user to input their email address, their password and their 2FA code in order to steal the user password.

Since there is no way for the user to authenticate the website (the normal 2FA is not mutual as it is with Cyphlens), the user would input all this information on the fake website and their password would be stolen without them noticing. Furthermore, without Cyphlens 2FA, it

would not help to have the 2FA step before the password as the outcome would be exactly the same: the password would be stolen. With Cyphlens 2FA, on the other hand, a phishing website would not be able to generate valid encrypted content that the user can decrypt and therefore it could never reach the password step as described above without giving away the fake nature of the phishing website.

In the description above Cyphlens 2FA images are shown to the user on a website. However, nothing prevents Cyphlens 2FA images to be sent to the user via SMS, in other mobile apps (e.g., WhatsApp), in emails or via other means, in order to complete the 2FA authentication process. Multiple channels may also be used simultaneously for an additional layer of security.

On top of the typical 2FA authentication functionalities, Cyphlens 2FA enables other advanced features based on things such as co-location, time duration, time of day, geo-location and user sharing. Let us look at each one of those.

Co-location: a Cyphlens 2FA image can be linked to a specific browser session so that if a user tries to log into a website from two different browsers or computers, he cannot use the Cyphlens 2FA information decrypted on computer 1 to authenticate on computer 2 and vice-versa, unless explicitly allowed by the Cyphlens 2FA configuration. Because of this, Cyphlens 2FA is effective also against password sharing and the sharing of 2FA codes which would not work on the other person's computer.

Time duration: Cyphlens 2FA images are valid for a configurable duration after which the encrypted content "expires" and the images cannot be decrypted any longer. Also, any information associated with the expired Cyphlens image is invalidated. This means that if I decrypt the Cyphlens 2FA image before its expiration and try to use the decrypted information after the expiration, the decrypted information will not be valid and the 2FA authentication will fail.

Time of day: Cyphlens 2FA images may be decrypted by a user only at/before/after a certain time of day. A user may receive a Cyphlens 2FA image via email at time  $t_0$ , for example, but would be able to decrypt this image and successfully complete the 2FA authentication only at time  $t_1$  with  $t_1 > t_0$ . At what time of day a Cyphlens 2FA image may be decrypted is programmable and configurable for the whole duration of the Cyphlens 2FA image lifecycle, even after its creation.

Geo-location: Cyphlens 2FA images may be decrypted by a user only if the user is at or within a certain distance from a specified location. This may imply that only the designated user can decrypt the Cyphlens 2FA image and complete the 2FA authentication if at that location. However, it may also imply that any user at that location may decrypt the Cyphlens 2FA image and complete the 2FA authentication. This could represent the first instance of a 2FA authentication in order to prove "where you are". Another way to do this, would be to include directly in the 2FA Cyphlens image some identifier of the location. A combination of both techniques is also possible. The geolocation at which a Cyphlens 2FA image can be decrypted and by whom, is programmable and configurable for the whole duration of the Cyphlens 2FA image lifecycle, even after its creation.

User sharing: in a typical 2FA scenario, the 2FA authentication step is linked to a single user (the owner of the second factor—something you have). This creates problems when a single account (e.g., an administrator account) with 2FA enabled, needs to be used by multiple users. In such a scenario, a user wanting to access the account needs to

contact the user owning the second factor and ask for the 2FA code or for approval. This is a very bad, and non-secure user experience as the exchange of the 2FA code or the authorization needs to happen in real time, when access to the account is required. With Cyphlens 2FA a user (owner) can decide to share its 2FA authentication for a certain amount of time or within a certain date interval with one or more users in parallel or sequentially. In doing so, those users will be able to decrypt the Cyphlens 2FA images of the owner and successfully complete the 2FA authentication without the need of any direct interaction with the owner. This is possible by creating Cyphlens 2FA images as shared images where a decryption key is associated to the Cyphlens image instead of being associated to a single user. Key distribution takes care of the rest.

Printed paper: in a typical 2FA application, the uses are primarily digital in nature. Cyphlens 2FA, on the other hand, can be extended to the physical medium (e.g., paper). For example, in order to decrypt some sensitive information encrypted in a printed Cyphlens image, a 2FA step may be required. In such a case, the second factor (something you have) can be a second Cyphlens image printed on paper. In order to decrypt the first image using the user mobile device, the user needs to place the second Cyphlens image (the second factor) in the vicinity of the first Cyphlens image that the user wants to decrypt. The mobile device will detect and "read" both printed images and only if the second factor image can be decrypted then the first image content can be unlocked and displayed to the user. This would allow the 2FA process to happen off-line without requiring any Internet access nor a network connection. In such a scenario, in order to "unlock" the content of the first Cyphlens image, a user must have physical access to the second-factor printed Cyphlens image and must be able to decrypt such second-factor Cyphlens image (owning the decryption keys). A double second-factor authentication.

Such a flow could be accomplished, for example, by encrypting in the second-factor Cyphlens image the secret key that is required to decrypt the first Cyphlens image. Many other variations of this flow are also possible where the second-factor Cyphlens image is printed while the first Cyphlens image is digital, or where a fully off-line user experience is not required and Internet access is available, for example.

When introducing elements of the present disclosure or the embodiments thereof, the articles "a," "an," and "the" are intended to mean that there are one or more of the elements. Similarly, the adjective "another," when used to introduce an element, is intended to mean one or more elements. The terms "including" and "having" are intended to be inclusive such that there may be additional elements other than the listed elements.

Although this invention has been described with a certain degree of particularity, it is to be understood that the present disclosure has been made only by way of illustration and that numerous changes in the details of construction and arrangement of parts may be resorted to without departing from the spirit and the scope of the invention.

What is claimed is:

1. A system for bidirectional two-factor remote user authentication, comprising:
  - a workflow engine comprising:
    - one or more processors; and
    - at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors, the at least one memory element retains login data;

a client device, the client device is in communication with the workflow engine over a network, the client device, comprising:  
 one or more processors;  
 at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors;  
 a display; and  
 a user login interface, the user login interface is configured to receive user identification data for login by the client device to a computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created, the one or more login identifiers are generated and encrypted by the workflow engine, wherein responsive to encryption, one or more encrypted login identifiers are visually encoded as an authentication image, the authentication image is displayed on the display of the client device;

an electronic device, the electronic device is in communication with the workflow engine over the network, the electronic device, comprising:  
 a display having a graphical user interface;  
 one or more processors;  
 at least one memory element, the at least one memory element stores the one or more login identifiers of the computer system and the user identification data; and  
 an authentication identifier reader, the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image, wherein responsive to decryption, one or more decrypted login identifiers and the user identification data are configured to be validated, by the workflow engine, to authenticate a user, and wherein one or more authenticated decrypted login identifiers are configured to be displayed on the display of the electronic device, and  
 an authorization for the login request for access to the computer system of the client device is configured to be transmitted, by the electronic device, to the workflow engine.

2. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image within a predetermined distance from a predetermined location.

3. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image at a predetermined time.

4. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the one or more encrypted login identifiers having encrypted content.

5. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image is a visual representation of the one or more encrypted login identifiers.

6. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the electronic device

having a camera, the camera is configured to capture the authentication image of the display of the client device.

7. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image of the display of the client device is uploaded to the electronic device.

8. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the user identification data is at least one of a username, an email address, or a password.

9. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the electronic device having an input sensor disposed on the display of the electronic device, the input sensor sensing an external input to submit the authorization for the login request to the workflow engine.

10. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authorization for the login request is transmitted to the workflow engine when the one or more authenticated decrypted login identifiers are input manually, by a user, into the computer system of the client device.

11. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the computer system of the client device is configured to prompt a user to input the user identification data into the computer system of the client device.

12. The system for the bidirectional two-factor remote user authentication of claim 1, further comprising a symmetric key is generated during a pairing, using transport layer security, before the authentication image is imported into the electronic device.

13. The system for the bidirectional two-factor remote user authentication of claim 1, further comprising public key infrastructure encryption of the one or more login identifiers and decryption of the one or more login identifiers from the authentication image.

14. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image is linked to a specific browser session.

15. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image is valid for a configurable duration, the authentication image and the user identification data is invalidated after the configurable duration has been exceeded.

16. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image is configured to be transmitted to the electronic device at time  $t_0$ , the authentication image is configured to be decrypted at time  $t_1$  with  $t_1 > t_0$ .

17. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image is configured to be decrypted when decryption is performed within a predetermined range of a predetermined location.

18. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image having geographical data.

19. The system for the bidirectional two-factor remote user authentication of claim 1, wherein the authentication image includes a shared authentication image having a decryption key.

20. A system for bidirectional two-factor remote user authentication, comprising:  
 a workflow engine comprising:  
 one or more processors; and

35

at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors, the at least one memory element retains login data;

an electronic device, the electronic device is in communication with the workflow engine over a network, the electronic device, comprising:

- one or more processors;
- at least one memory element, the at least one memory element configured to store instructions for controlling the one or more processors;
- a display; and
- a user login interface, the user login interface is configured to receive user identification data for login by the electronic device to a computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created, the at least one memory element is configured to store the one or more login identifiers of the computer system and the user identification data, the one or more login identifiers are generated and encrypted by the workflow engine, wherein
  - responsive to encryption, one or more encrypted login identifiers are visually encoded as an authentication image, the authentication image is displayed on the display of the electronic device; and
  - an authentication identifier reader, the authentication identifier reader is configured to decrypt the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image, wherein
    - responsive to decryption, one or more decrypted login identifiers and the user identification data are configured to be validated, by the workflow engine, to authenticate a user, and wherein

36

one or more authenticated decrypted login identifiers are configured to be displayed on the display of the electronic device, and

an authorization for the login request for access to the computer system of the electronic device is configured to be transmitted, by the electronic device, to the workflow engine.

21. A method for mutual two-factor remote user authentication, comprising:

- receiving, at a workflow engine, a request for a login of a client device to a computer system from a user login interface, the user login interface is configured to receive user identification data for login by the client device to the computer system, the computer system having one or more login identifiers identifying the user login interface at which a login request is created;
- responsive to the request from the client device, the workflow engine generating one or more login identifiers;
- encrypting, by the workflow engine, the one or more login identifiers;
- responsive to encrypting, visually encoding the one or more login identifiers as an authentication image by the workflow engine;
- decrypting, using an authentication identifier reader, the one or more login identifiers from the authentication image when the authentication identifier reader identifies the authentication image;
- responsive to decryption, validating by the workflow engine, one or more decrypted login identifiers and the user identification data to authenticate a user; and
- transmitting an authorization to the workflow engine for the login request for access to the computer system of the client device.

\* \* \* \* \*