complete a transaction. However, if the log-in credentials are compromised, another person could have access to the user's account.

[0005] Accordingly, there is a need to improve authentication mechanisms for account access and the competition of transactions, including payment transactions.

SUMMARY

[0006] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for utilizing a steganographically encoded image to verify a user and/or complete a transaction, including but not limited to a payment transaction. According to one or more examples, an online or offline protocol is used to verify and/or authenticate a user in order to initiate an exchange of information that utilizes the steganographic image for authentication.

[0006a] According to a first aspect of the present invention, there is provided a method, comprising:

performing at least one verification operation by an application executing on a processor of a client device in communication with a contactless card using near field communication (NFC);

responsive to performing the at least one verification operation, receiving, by the client device from the contactless card, a steganographic image, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template; and

authenticating a user associated with the client device based on the steganographic image.

[0006b] According to a second aspect of the present invention, there is provided an apparatus, comprising:

a processor circuit; and

a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

perform at least one verification operation by an application executing on the processor circuit in communication with a contactless card using near field communication (NFC); and

responsive to performing the at least one verification operation, receive, by the application from the contactless card, a steganographic image to authenticate a user, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template.

[0006c] According to a third aspect of the present invention, there is provided a computer-readable storage medium comprising computer-readable instructions executable by a processor circuit to cause the processor circuit to:

perform at least one verification operation by an application executing on the processor circuit in communication with a contactless card using near field communication (NFC); and

responsive to performing the at least one verification operation, receive, by the application from the contactless card, a steganographic image to authenticate a user, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template.

[0007] There is disclosed a computer implemented method utilizing application executing on a computer system may initiate a transaction to verify an identity of a user and/or authorizing a transaction using a steganographically encoded image. In various embodiments, the application may be launched by tapping the contactless card on a user device, e.g. a mobile device. The method can include: communicating, by an application executing on a processor circuit associated with a computer device of the user and using near field communication (NFC), with the contactless card, the contactless card having a radio frequency identification (RFID) chip, and the contactless card being within an NFC range of the digital reader associated with the third-party device, performing at least one verification operation by the application and in communication with the contactless card, responsive to performing the at least one verification operation and in communication with the contactless card, receiving a steganographic image to

authenticate a user associated with the computer device, wherein the steganographic image includes a government issued identification of a user steganographically encoded with a fingerprint template of the user, wherein the steganographic image is created by: certifying the image of the identification of the user as authentic at a verification device, and creating the steganographic image at the verification device after certification.

[0008] There is disclosed a system employing online and/or offline authentication and the steganographically encoded image to authenticate and/or verify a user and/or authorize a transaction. The system can include: a processor circuit, and a memory storing instructions which when executed by the processor circuit, cause the processor circuit to: receive, by an application executing on a processor circuit associated with a computer device and from a user, a first application user credential associated with a user profile, compare, for a first match and by the processor associated with the application, the first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity, and responsive to finding the first match, authenticate an identity of a user by initiating a communication with a communication interface of a contactless card, the communication including performing i) at least one of a) a host-less verification operation and b) an issuer based verification operation and ii) an exchange of information that includes an image of a government identification of the user, the image including a steganographically encoding of a fingerprint template associated with the user.

[0009] There is disclosed a contactless card with a communication interface for communicating with a computing device, and a processing circuitry for storing information is provided, where the information includes an identification image of a user, where the identification image is steganographically encoded with a fingerprint template associated with the user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Figure 1 illustrates an embodiment of a system for verifying or authenticating a user according to a payment protocol.

[0011] Figure 2 illustrates at least one embodiment of tapping to verify a user utilizing an authentication protocol.

CLAIMS

1. A method, comprising:

performing at least one verification operation by an application executing on a processor of a client device in communication with a contactless card using near field communication (NFC);

responsive to performing the at least one verification operation, receiving, by the client device from the contactless card, a steganographic image, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template; and

authenticating a user associated with the client device based on the steganographic image.

2. The method of claim 1, further comprising:

creating the steganographic image based on a certification of the image of the government issued identification, wherein the certification certifies the image of the government issued identification as authentic.

3. The method of claim 1, wherein the authenticating comprises:

receiving, from a scanning device, a fingerprint scan of a finger of the user;

extracting a scanned fingerprint template from the fingerprint scan; and

comparing the scanned fingerprint template to the received fingerprint template for a match.

4. The method of claim 1, wherein performing the at least one verification operation comprises:

receiving, by the application from the contactless card, a public key of a key pair of the contactless card and a user identification, the user identification including the steganographic image;

instructing, by the application, generation of a digital signature by the card using a private key of the key pair of the card;

receiving the digital signature from the card; and

verifying the digital signature using the public key.

5. The method of claim 4, further comprising:

comparing a first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity, wherein the performing of the at least one verification operation is responsive finding a match between the first application user credential and the stored second application user credential.

6. The method of claim 4, wherein performing the at least one verification operation further comprises:

determining if a transaction associated with NFC communication with a transaction device exceeds a monetary threshold amount; and

if the transaction exceeds the monetary threshold amount, perform an additional security confirmation measure, and

if the transaction does not exceed the monetary threshold amount, receive a message that the user has been authenticated at the transaction device.

7. The method of claim 6, wherein performing the additional security confirmation measure comprises:

scanning a finger of the user associated with the fingerprint template using a scanning device to extract a scanned fingerprint template from the user;

transmitting the scanned fingerprint template and the received fingerprint template to a server;

comparing, at the server, the scanned fingerprint template to the received fingerprint template for a match; and

receiving, at the transaction device and from the server, an indication confirming the match.

8. The method of claim 1,wherein performing the at least one verification operation comprises:

determining, by the application, that the user has initiated a transaction with a transaction device to identify the user;

receiving, by the application, encrypted data from the contactless card, the encrypted data generated based a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card and generated based on a master key and a counter value stored in the memory of the contactless card;

transmitting, by the application, the encrypted data to a server;

receiving, by the application from the server, verification of the encrypted data, the server to decrypt the encrypted data based on the cryptographic algorithm and the diversified key stored in a memory of the server to verify the encrypted data, the diversified key stored in the memory of the server generated based on a master key and a counter value stored in the memory of the server; and

receiving, by the application from the server, the steganographic image from the server.

9. An apparatus, comprising:

a processor circuit; and

a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

perform at least one verification operation by an application executing on the processor circuit in communication with a contactless card using near field communication (NFC); and

responsive to performing the at least one verification operation, receive, by the application from the contactless card, a steganographic image to authenticate a user, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template.

10. The apparatus of claim 9, wherein the steganographic image is based on a certification of the image of the government issued identification, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive, from a scanning device, a fingerprint scan of a finger of the user;

extract a scanned fingerprint template from the fingerprint scan; and

determine, based on a comparison, that the scanned fingerprint template and the received fingerprint template match to authenticate the user.

11. The apparatus of claim 10, wherein the instructions to perform the at least one verification operation comprise instructions to:

receive, by the application from the contactless card, a public key of a key pair of the contactless card and a user identification, the user identification including the steganographic image;

receive, by the application, a digital signature generated by the card using a private key of the key pair of the card; and

verify the digital signature using the public key.

12. The apparatus of claim 11, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

compare a first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity, wherein the performing of the at least one verification operation is responsive finding a match between the first application user credential and the stored second application user credential.

13. The apparatus of claim 9, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive, by the application and from the contactless card, a public key of a key pair of the contactless card and a user identification, the user identification including the steganographic image;

receive, by the application, a digital signature generated by the card using a private key of the key pair of the card;

verify the digital signature using the public key;

determining if a transaction associated with NFC communication with a transaction device exceeds a monetary threshold amount; and

if the transaction exceeds the monetary threshold amount, perform an additional security confirmation measure, and

if the transaction does not exceed the monetary threshold amount, receive a message that the user has been authenticated at the transaction device.

14. The apparatus of claim 9, wherein the instructions to perform the at least one verification operation comprise instructions to:

determine, by the application, that the user has initiated a transaction with a transaction device to identify the user;

receive, by the application, encrypted data from the contactless card, the encrypted data based on a cryptographic algorithm and a diversified key, the diversified key based on a master key and a counter value;

transmit, by the application, the encrypted data to a server;

receive, by the application from the server, verification of the encrypted data, the server to decrypt the encrypted data based on an instance of the diversified key to verify the encrypted data; and

receive, by the application from the server, the steganographic image from the server.

15. A computer-readable storage medium comprising computer-readable instructions executable by a processor circuit to cause the processor circuit to:

perform at least one verification operation by an application executing on the processor circuit in communication with a contactless card using near field communication (NFC); and

responsive to performing the at least one verification operation, receive, by the application from the contactless card, a steganographic image to authenticate a user, wherein the steganographic image includes an image of a government issued identification steganographically encoded with a fingerprint template.

16. The computer-readable storage medium of claim 15, wherein the steganographic image is based on a certification of the image of the government issued identification, the medium comprising instructions executable by the processor circuit to cause the processor circuit to:

receive, from a scanning device, a fingerprint scan of a finger of the user;

extract a scanned fingerprint template from the fingerprint scan; and

determine, based on a comparison, that the scanned fingerprint template and the received fingerprint template match to authenticate the user.

17. The computer-readable storage medium of claim 16, the instructions to perform the at least one verification comprising instructions to:

receive, by the application from the contactless card, a public key of a key pair of the contactless card and a user identification, the user identification including the steganographic image;

receive, by the application, a digital signature generated by the card using a private key of the key pair of the card; and

verify the digital signature using the public key.

18. The computer-readable storage medium of claim 17, comprising instructions executable by the processor circuit to cause the processor circuit to:

compare a first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity, wherein the performing of the at least one verification operation is responsive finding a match between the first application user credential and the stored second application user credential.

19. The computer-readable storage medium of claim 15, the instructions to perform the at least one verification comprising instructions to:

receive, by the application and from the contactless card, a public key of a key pair of the contactless card and a user identification, the user identification including the steganographic image;

instruct, by the application, generation of a digital signature by the card using a private key of the key pair of the card;

receive the digital signature from the card;

verify the digital signature using the public key;

determine if a transaction associated with NFC communication with a transaction device exceeds a monetary threshold amount; and

if the transaction exceeds the monetary threshold amount, perform an additional security confirmation measure, and

if the transaction does not exceed the monetary threshold amount, receive a message that the user has been authenticated at the transaction device.

20. The computer-readable storage medium of claim 15, the instructions to perform the at least one verification comprising instructions to:

determine, by the application, that the user has initiated a transaction with a transaction device to identify the user;

receive, by the application, encrypted data from the contactless card, the encrypted data based on a cryptographic algorithm and a diversified key, the diversified key based on a master key and a counter value;

transmit, by the application, the encrypted data to a server;

receive, by the application from the server, verification of the encrypted data, the server to decrypt the encrypted data based on an instance of the diversified key to verify the encrypted data; and

receive, by the application from the server, the steganographic image from the server.