

CLAIMS

What is claimed is:

1. A method of distributing customized privacy-preserving images to a plurality of users, the method comprising employing at least one hardware processor of a privacy management server to:
 - in response to receiving an encrypted source image decryptable with an administration key, perform an encrypted-domain image segmentation of the source image to produce a plurality of user-specific encrypted private images, wherein:
 - a selected private image comprises a region of the source image selected to show a private item of a selected user of the plurality of users, and
 - another private image comprises another region of the source image selected to show a private item of another user of the plurality of users;
 - in response to the image segmentation, perform an encrypted-domain key change procedure to produce a plurality of user-specific re-encrypted images, wherein:
 - a selected re-encrypted image comprises a result of transforming the selected private image from being decryptable with the administration key to being decryptable with a private key of the selected user, and
 - another re-encrypted image comprises a result of transforming the other private image from being decryptable with the administration key to being decryptable with a private key of the other user; and
 - transmit the plurality of user-specific re-encrypted images to an image distribution server for further distribution to client devices configured to reconstruct user-specific plaintext versions of the source image.
2. The method of claim 1, wherein:
 - performing the encrypted-domain image segmentation of the source image further comprises determining an encrypted public image comprising regions of

4 the source image selected to show neither the private item of the selected
5 user nor the private item of the other user;
6 wherein the method further comprises employing at least one hardware processor
7 of the privacy management server to transmit the encrypted public image
8 to the image distribution server for decryption and further distribution to
9 client devices; and
10 wherein the client devices are configured to reconstruct user-specific plaintext
11 versions of the source image further according to a decrypted public image
12 received from the image distribution server.
13

1 3. The method of claim 1, further comprising employing at least one hardware processor
2 of the image distribution server to:
3 in response to receiving the selected re-encrypted image, select a device from a
4 plurality of client devices according to whether the selected device is
5 operated by the selected user; and
6 in response to selecting the client device, transmit the selected re-encrypted image
7 to the selected device.
8

1 4. The method of claim 3, further comprising employing at least one hardware
2 processor of the image distribution server to:
3 in response to receiving the other re-encrypted image, select another
4 device from the plurality of client devices according to whether the
5 other device is operated by the other user; and
6 in response to selecting the other device, transmit the other re-encrypted
7 image to the other device.
8

1 5. The method of claim 1, wherein determining the selected private image comprises:
2 employing a pre-trained item detector to calculate a mask identifying the region of
3 the source image showing the private item of the selected user, the mask

- 4 calculated in the encrypted domain and decryptable with the
5 administration key; and
6 determining the selected private image according to a pixel-wise multiplication of
7 the encrypted source image and the mask.
8
- 1 6. The method of claim 1, wherein the encrypted source image is encrypted according to
2 a homomorphic encryption scheme.
3
- 1 7. The method of claim 1, wherein a plaintext version of the source image reconstructed
2 by a client device operated by the selected user shows the private item of the
3 selected user and obscures the private item of the other user.
4
- 1 8. The method of claim 1, wherein the private item comprises an item selected from a
2 group consisting of a person and a human face.
3
- 1 9. The method of claim 1, wherein the private item comprises a bank card.
2
- 1 10. The method of claim 1, wherein the private item comprises a trademark.
2
- 1 11. A computer system comprising a privacy management server configured to:
2 in response to receiving an encrypted source image decryptable with an administration
3 key, perform an encrypted-domain image segmentation of the source image to
4 produce a plurality of user-specific private images, wherein:
5 a selected private image comprises a region of the source image selected to show
6 a private item of a selected user of the plurality of users, and
7 another private image comprises another region of the source image selected to
8 show a private item of another user of the plurality of users;
9 in response to the image segmentation, perform an encrypted-domain key change
10 procedure to produce a plurality of user-specific re-encrypted images, wherein:

11 a selected re-encrypted image comprises a result of transforming the selected
12 private image from being decryptable with the administration key to being
13 decryptable with a private key of the selected user, and
14 another re-encrypted image comprises a result of transforming the other private
15 image from being decryptable with the administration key to being
16 decryptable with a private key of the other user; and
17 transmit the plurality of user-specific re-encrypted images to an image distribution
18 server for further distribution to client devices configured to reconstruct
19 user-specific plaintext versions of the source image.
20

1 12. The computer system of claim 11, wherein:

2 performing the encrypted-domain image segmentation of the source image further
3 comprises determining an encrypted public image comprising regions of
4 the source image selected to show neither the private item of the selected
5 user nor the private item of the other user;
6 wherein the privacy management server is further configured to transmit the
7 encrypted public image to the image distribution server for decryption and
8 further distribution to client devices; and
9 wherein the client devices are configured to reconstruct user-specific plaintext
10 versions of the source image further according to a decrypted public image
11 received from the image distribution server.
12

1 13. The computer system of claim 11, further comprising the image distribution server
2 and wherein the image distribution server is further configured to:

3 in response to receiving the selected re-encrypted private image, select a device
4 from a plurality of client devices according to whether the selected device
5 is operated by the selected user; and
6 in response to selecting the client device, transmit the selected re-encrypted
7 private image to the selected device.

8

1

14. The computer system of claim 13, wherein the image distribution server is further configured to:

2

3

in response to receiving the other re-encrypted private image, select

4

another device from the plurality of client devices according to

5

whether the other device is operated by the other user; and

6

in response to selecting the other device, transmit the other re-encrypted private image to the other device.

7

8

1

15. The computer system of claim 11, wherein determining the selected private image comprises:

2

3

employing a pre-trained item detector to calculate a mask identifying the region of

4

the source image showing the private item of the selected user, the mask

5

calculated in the encrypted domain and decryptable with the

6

administration key; and

7

determining the selected private image according to a pixel-wise multiplication of the encrypted source image and the mask.

8

9

1

16. The computer system of claim 11, wherein the encrypted source image is encrypted according to a homomorphic encryption scheme.

2

3

1

17. The computer system of claim 11, wherein a plaintext version of the source image reconstructed by a client device operated by the selected user shows the private item of the selected user and obscures the private item of the other user.

2

3

4

1

18. The method of claim 1, wherein the private item comprises an item selected from a group consisting of a person and a human face.

2

3

1

19. The computer system of claim 11, wherein the private item comprises a bank card.

2
1
2
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

20. The computer system of claim 11, wherein the private item comprises a trademark.

21. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a privacy management server, cause the privacy management server to:
- in response to receiving an encrypted source image decryptable with an administration key, perform an encrypted-domain image segmentation of the source image to produce a plurality of user-specific private images, wherein:
- a selected private image comprises a region of the source image selected to show a private item of a selected user of the plurality of users, and
- another private image comprises another region of the source image selected to show a private item of another user of the plurality of users;
- in response to the image segmentation, perform an encrypted-domain key change procedure to produce a set of user-specific re-encrypted images, wherein:
- a selected re-encrypted image comprises a result of transforming the selected private image from being decryptable with the administration key to being decryptable with a private key of the selected user, and
- another re-encrypted image comprises a result of transforming the other private image from being decryptable with the administration key to being decryptable with a private key of the other user; and
- transmit the plurality of user-specific re-encrypted images to an image distribution server for further distribution to client devices configured to reconstruct user-specific plaintext versions of the source image.