

CLAIMS

What is claimed is:

1. A method of distributing 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 determine a plurality of encrypted private masks, each mask of the plurality of encrypted private masks indicating a region of the source image selected to show a private item of a respective user of the plurality of users;
 - transmit the plurality of encrypted private masks to an image distribution server for decryption;
 - in response, determine a plurality of encrypted private images, each private image of the plurality of encrypted private images determined according to the source image and further according to a respective decrypted mask comprising a decryption of a respective mask of the plurality of encrypted private masks, the respective decrypted mask received from the image distribution server;
 - perform an encrypted-domain key change procedure to generate a plurality of re-encrypted images, each re-encrypted image of the plurality of re-encrypted images comprising a result of transforming a respective private image of the plurality of encrypted private images from being decryptable with the administration key to being decryptable with a private key of the respective user;
 - combine the plurality of re-encrypted images into a composite private image; and
 - transmit the composite private image to the image distribution server for further distribution to a plurality of client devices, wherein each client device is configured to reconstruct a user-specific plaintext version of the source image according to the composite private image.

26

1 2. The method of claim 1, comprising determining the each private image according to:

$$2 \quad I^* \odot M,$$

3 wherein the circled dot symbol denotes pixel-wise multiplication, I^* denotes the
4 encrypted source image, and M denotes the respective decrypted mask.

5

1 3. The method of claim 1, wherein combining the plurality of re-encrypted images
2 comprises copying the each re-encrypted image into the composite private image
3 at a location indicated by the respective decrypted mask.

4

1 4. The method of claim 1, comprising determining the composite private image
2 according to a pixel-wise addition of the plurality of the re-encrypted images.

3

1 5. The method of claim 1, 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 no private items of any user of the
5 plurality of users;

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 distribution server for decryption and further transmission to the
9 plurality of client devices; and

10 wherein the each client device is configured to reconstruct the user-specific
11 plaintext version of the source image further according to a decrypted
12 public image received from the image distribution server.

13

1 6. The method of claim 5, comprising determining the encrypted public image
2 according to the respective decrypted mask.

3

- 1 7. The method of claim 1, wherein the encrypted source image is encrypted according to
2 a homomorphic encryption scheme.
3
- 1 8. The method of claim 1, wherein the plaintext version of the source image shows a
2 private item of a selected user of the plurality of users and obscures private items
3 of other users of the plurality of users.
4
- 1 9. The method of claim 1, wherein the private item comprises an item selected from a
2 group consisting of a person and human face.
3
- 1 10. The method of claim 1, wherein the private item comprises a bank card.
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 determine a plurality of encrypted private masks, each mask of the plurality of
5 encrypted private masks indicating a region of the source image selected to show
6 a private item of a respective user of the plurality of users;
7 transmit the plurality of encrypted private masks to an image distribution server for
8 decryption;
9 in response, determine a plurality of encrypted private images, each private image of the
10 plurality of encrypted private images determined according to the source image
11 and further according to a respective decrypted mask comprising a decryption of a
12 respective mask of the plurality of encrypted private masks, the respective
13 decrypted mask received from the image distribution server;
14 perform an encrypted-domain key change procedure to generate a plurality of re-
15 encrypted images, each re-encrypted image of the plurality of re-encrypted
16 images comprising a result of transforming a respective private image of the

plurality of encrypted private images from being decryptable with the administration key to being decryptable with a private key of the respective user; combine the plurality of re-encrypted images into a composite private image; and transmit the composite private image to the image distribution server for further distribution to a plurality of client devices, wherein each client device is configured to reconstruct a user-specific plaintext version of the source image according to the composite private image.

12. The computer system of claim 11, wherein the privacy management server is configured to determine the each private image according to:

$$I^* \odot M,$$

wherein the circled dot symbol denotes pixel-wise multiplication, I^* denotes the encrypted source image, and M denotes the respective decrypted mask.

13. The computer system of claim 11, wherein combining the plurality of re-encrypted images comprises copying the each re-encrypted image into the composite private image at a location indicated by the respective decrypted mask.

14. The computer system of claim 11, wherein the privacy management server is configured to determine the composite private image according to a pixel-wise addition of the plurality of the re-encrypted images.

15. The computer system of claim 11, wherein:

performing the encrypted-domain image segmentation of the source image further comprises determining an encrypted public image comprising regions of the source image selected to show no private items of any user of the plurality of users;

6 wherein the privacy management server is further configured to transmit the
7 encrypted public image to the distribution server for decryption and
8 further transmission to the plurality of client devices; and
9 wherein the each client device is configured to reconstruct the user-specific
10 plaintext version of the source image further according to a decrypted
11 public image received from the image distribution server.
12

1 16. The computer system of claim 15, wherein the privacy management server is
2 configured to determine the encrypted public image according to the
3 respective decrypted mask.
4

1 17. The computer system of claim 11, wherein the encrypted source image is encrypted
2 according to a homomorphic encryption scheme.
3

1 18. The computer system of claim 11, wherein the plaintext version of the source image
2 shows a private item of a selected user of the plurality of users and obscures
3 private items of other users of the plurality of users.
4

1 19. The computer system of claim 11, wherein the private item comprises an item
2 selected from a group consisting of a person and human face.
3

1 20. The computer system of claim 11, wherein the private item comprises a bank card.
2

1 21. A non-transitory computer-readable medium storing instructions which, when executed
2 by at least one hardware processor of a privacy management server, cause the privacy
3 management server to:
4 in response to receiving an encrypted source image decryptable with an administration
5 key, perform an encrypted-domain image segmentation of the source image to
6 determine a plurality of encrypted private masks, each mask of the plurality of

7 encrypted private masks indicating a region of the source image selected to show
8 a private item of a respective user of the plurality of users;
9 transmit the plurality of encrypted private masks to an image distribution server for
10 decryption;
11 in response, determine a plurality of encrypted private images, each private image of the
12 plurality of encrypted private images determined according to the source image
13 and further according to a respective decrypted mask comprising a decryption of a
14 respective mask of the plurality of encrypted private masks, the respective
15 decrypted mask received from the image distribution server;
16 perform an encrypted-domain key change procedure to generate a plurality of re-
17 encrypted images, each re-encrypted image of the plurality of re-encrypted
18 images comprising a result of transforming a respective private image of the
19 plurality of encrypted private images from being decryptable with the
20 administration key to being decryptable with a private key of the respective user;
21 combine the plurality of re-encrypted images into a composite private image; and
22 transmit the composite private image to the image distribution server for further
23 distribution to a plurality of client devices, wherein each client device is
24 configured to reconstruct a user-specific plaintext version of the source image
25 according to the composite private image.
26