Claims

1. An image privacy protection method, comprising:

performing privacy content recognition on an original image;

in response to a privacy content being recognized, determining a local region including the privacy content from the original image;

performing privacy protection processing on image data for the local region to generate data of a privacy-protected original image, the privacy protection processing including image scrambling processing, wherein the privacy protection processing includes encrypting the image data for the local region by using a nonlinear hyperchaotic system to obtain encrypted image data, and superimposing the encrypted image data and the original image data; and

performing image compression processing on the data of the privacy-protected original image to generate data of a compressed image, and using the data of the compressed image as image data to be transmitted or stored.

2. The method according to claim 1, wherein the performing the privacy content recognition on the original image includes at least one of:

performing facial recognition on the original image, and in response to a face image being recognized, using the face image as the privacy content; or

performing semantic analysis on text information of the original image, and in response to an analysis result of the semantic analysis being relevant to a user's privacy information, using the text information as the privacy content.

3. The method according to claim 1, wherein the performing the privacy protection processing on the image data for the local region further includes

rearranging a data order of the image data for the local region to obtain obfuscated image data.

4. The method according to claim 3, wherein the performing the privacy protection processing further includes performing image obfuscation processing on the image data for the local region or on the first scrambled image data, wherein performing the image obfuscation processing on the image data for the local region or on the scrambled image data generated based on the image data for the local region includes using a predetermined obfuscation circuit.

5. The method according to claim 2, wherein the determining the local region including the privacy content from the original image includes:

determining a location of the privacy content from the original image; and

determining, from the original image based on the location of the privacy content, at least one non-overlapped local region that includes the privacy content on the whole.

6. The method according to claim 5, wherein the determining, from the original image based on the location of the privacy content, the at least one non-overlapped local region that includes the privacy content on the whole includes: in response to the privacy content being one or more face images, forming a closed region through boundaries of a location of each face image on the original image, and using a regular-pattern region including the closed region in the original image as a local region, each local region including only one closed region.

7. The method according to claim 5, wherein: in response to at least two non-overlapped local regions being determined from the original image as including the privacy content, respective image data of non-overlapped local regions of the at least two non-overlapped local regions are processed differently in at least one of the image scrambling processing or in image obfuscation processing in the privacy protection processing.

8. The method according to claim 1, wherein the performing the image compression processing on the data of the privacy-protected original image to generate the data of the compressed image includes:

performing overall encryption processing on the data of the privacy-protected original image to generate data of overall encrypted original image, and

performing the image compression processing on the data of the overall encrypted original image.

9. An image privacy protection apparatus, comprising:

a content recognition module, configured to perform privacy content recognition on an original image;

a region determining module, configured to, in response to a privacy content being recognized, determine a local region including the privacy content from the original image;

an image processing module, configured to perform privacy protection processing on image data for the local region to generate data of a privacy-protected original image, the privacy protection processing including image scrambling processing, wherein the privacy protection processing includes encrypting the image data for the local region by using a nonlinear hyperchaotic system to obtain encrypted image data, and superimposing the encrypted image data and the original image data; and

an image compression module, configured to perform image compression processing on the data of the privacy-protected original image to generate data of a compressed image, and use the compressed image as image data to be transmitted or stored.

10. An image privacy protection device, comprising:

a processor; and

a memory storing computer-executable instructions that, when executed by the processor, enable the processor to implement acts including:

performing privacy content recognition on an original image;

in response to a privacy content being recognized, determining a local region including the privacy content from the original image;

performing privacy protection processing on image data for the local region to generate data of a privacy-protected original image, the privacy protection processing including image scrambling processing, wherein the privacy protection processing includes encrypting the image data for the local region by using a nonlinear hyperchaotic system to obtain encrypted image data, and superimposing the encrypted image data and the original image data; and

performing image compression processing on the data of the privacy-protected original image to generate data of a compressed image, and using the data of the compressed image as image data to be transmitted or stored.

11. The device according to claim 10, wherein the performing the privacy content recognition on the original image includes at least one of:

performing facial recognition on the original image, and in response to a face image being recognized, using the face image as the privacy content; or

performing semantic analysis on text information of the original image, and in response to an analysis result of the semantic analysis being relevant to a user's privacy information, using the text information as the privacy content.

12. The device according to claim 10, wherein the performing the privacy protection processing on the image data for the local region further includes

rearranging a data order of the image data for the local region to obtain obfuscated image data.

13. The device according to claim 12, wherein the performing the privacy protection processing further includes performing image obfuscation processing on the image data for the local region or on the first scrambled image data, wherein performing the image obfuscation

processing on the image data for the local region or on the scrambled image data generated based on the image data for the local region includes using a predetermined obfuscation circuit.

14. The device according to claim 11, wherein the determining the local region including the privacy content from the original image includes:

determining a location of the privacy content from the original image; and

determining, from the original image based on the location of the privacy content, at least one non-overlapped local region that includes the privacy content on the whole.

15. The device according to claim 14, wherein the determining, from the original image based on the location of the privacy content, the at least one non-overlapped local region that includes the privacy content on the whole includes: in response to the privacy content being one or more face images, forming a closed region through boundaries of a location of each face image on the original image, and using a regular-pattern region including the closed region in the original image as a local region, each local region including only one closed region.

16. The device according to claim 14, wherein: in response to at least two non-overlapped local regions being determined from the original image as including the privacy content, respective image data of non-overlapped local regions of the at least two non-overlapped local regions are processed differently in at least one of the image scrambling processing or in image obfuscation processing in the privacy protection processing.

17. The device according to claim 10, wherein the performing the image compression processing on the data of the privacy-protected original image to generate the data of the compressed image includes:

performing overall encryption processing on the data of the privacy-protected original image to generate data of overall encrypted original image, and

performing the image compression processing on the data of the overall encrypted original image.

18. A storage medium having computer-executable instructions stored thereon that, when executed by a processor, configure the processor to implement acts including:

performing privacy content recognition on an original image;

in response to a privacy content being recognized, determining a local region including the privacy content from the original image;

performing privacy protection processing on image data for the local region to generate data of a privacy-protected original image, the privacy protection processing including image scrambling processing, wherein the privacy protection processing includes encrypting the image data for the local region by using a nonlinear hyperchaotic system to obtain encrypted image data, and superimposing the encrypted image data and the original image data; and

performing image compression processing on the data of the privacy-protected original image to generate data of a compressed image, and using the compressed image as image data to be transmitted or stored.