

THE INVENTION CLAIMED IS

1. A computer-implemented method for obfuscating at least one sensitive datum on at least one surface of a captured credential in the course of an interaction, the method comprising:

determining, with at least one processor, whether image data associated with an interaction has the at least one sensitive datum on the at least one surface;

in response to determining that the image data has the at least one sensitive datum on the at least one surface, determining, with the at least one processor, at least one image data region occupied by the at least one sensitive datum,

applying at least one obfuscation operation to the at least one image data region, wherein the at least one obfuscation operation renders the at least one sensitive datum unreadable by a human or a machine, and wherein the at least one obfuscation operation is based on an application for which the credential is being used; and

generating and outputting a resulting obfuscated image of the at least one surface of the credential.

2. The computer-implemented method of claim 1, wherein determining the image data region occupied by the at least one sensitive datum comprises:

locating within the image data, with the at least one processor, at least one edge of the at least one sensitive datum; and

connecting the at least one edge to at least one other edge, with the at least one processor, to establish at least one boundary of the at least one sensitive datum;

wherein the at least one obfuscation operation is applied to the image data bounded by at least one boundary.

3. The computer-implemented method of claim 1, further comprising applying at least one face detection operation to detect and isolate the at least one

sensitive datum within the image data, wherein the image data comprises a photo of a user to be obfuscated.

4. The computer-implemented method of claim 3, wherein the at least one face detection operation comprises a Viola-Jones face detector, a boost-based face detection scheme, a Haar feature extractor, a neural network solution, or any combinations thereof.

5. The computer-implemented method of claim 1, further comprising applying at least one OCR operation to the image data to detect and isolate the at least one sensitive datum within the image data, wherein the at least one sensitive datum comprises at least one alphanumeric character.

6. The computer-implemented method of claim 5, wherein the OCR operation comprises at least one pre-processing operation, one character recognition operation, or one post-processing operation, or any combination thereof.

7. The computer-implemented method of claim 2, further comprising using an edge detection algorithm to establish the at least one edge of the at least one sensitive datum and to connect the at least one of the edges of the at least one sensitive datum to establish the at least one boundary of the at least one sensitive datum.

8. The computer-implemented method of claim 1, wherein the obfuscation operation comprises blurring, masking, pixilation, or any combination thereof.

9. The computer-implemented method of claim 2, wherein the at least one image data region comprises at least one of the following: at least one photo detected within the at least one image data region, at least one block of contiguous OCR isolated characters within the image data region, at least one row comprising at least one block of OCR isolated characters within the image data region, or any combination thereof.

10. The computer-implemented method of claim 1, wherein performing the image processing operation comprises at least one of the following:

- performing a subsampling operation on the image data;
- performing an image segmentation locating the at least one sensitive datum;
- performing an edge detection operation on the image data containing the at least one sensitive datum;
- performing an operation that bounds the at least one sensitive datum;
- performing at least one face detection operation on the image data;
- performing at least one OCR operation on the image data;
- performing at least one blurring operation on the image data containing the at least one sensitive datum;
- performing at least one masking operation on the image data containing the at least one sensitive datum;
- performing at least one pixelation operation on the image data containing the at least one sensitive datum;
- performing at least one image generation and/or output operation; or
- any combination thereof.

11. A system for obfuscating at least one sensitive datum on at least one surface of a captured credential in the course of an interaction, the system comprising at least one processor, wherein the at least one processor is programmed or configured for:

- determining whether image data associated with the credential has at least one sensitive datum on the at least one surface;

- in response to determining that the image data has the at least one sensitive datum on the at least one surface, applying at least one obfuscation operation to the at least one sensitive datum, wherein the at least one obfuscation operation renders the at least one sensitive datum unreadable by a human or a machine, wherein the at least one obfuscation operation is based on an application for which the credential is being used; and

- generating and outputting a resulting obfuscated image of the at least one surface of the credential.

12. The system of claim 11, wherein the at least one processor is further programmed or configured for:

determining the image data region occupied by the at least one sensitive datum by locating within the image data the location of at least one edge of the at least one sensitive datum;

connecting the at least one edge comprising the perimeter of the at least one sensitive datum to establish a boundary of the at least one sensitive datum;

applying the at least one obfuscation operation to the image data bounded by the established boundary; and

generating and output a resulting obfuscated image of the at least one surface of the credential for storage, display or any combination thereof.

13. The system of claim 11, wherein the at least one processor is further programmed or configured to apply at least one face detection operation to detect and isolate the at least one sensitive datum within the image data that may be a photo of a user to be obfuscated.

14. The system of claim 13, wherein the at least one face detection operation comprises Viola-Jones face detector, a boost-based face detection scheme, a Haar feature extractor, a neural network solution, or any combination thereof.

15. The system of claim 11, wherein the at least one processor is further programmed or configured for applying at least one OCR operation to the image data to detect and isolate the at least one sensitive datum within the image data that comprises at least one alphanumeric character.

16. The system of claim 15, wherein the OCR operation comprises at least one pre-processing operation, one character recognition operation, or one post-processing operation, or any combination thereof.

17. The system of claim 11, wherein the at least one processor is programmed or configured for establishing the at least one edge of the at least one sensitive datum and to connect the at least one edge of the at least one sensitive datum to establish the at least one boundary of the at least one sensitive datum.

18. The system of claim 11, wherein the at least one processor is programmed or configured for applying at least one obfuscation operation comprising blurring, masking, pixilation, or any combination thereof.

19. The system of claim 11, wherein the at least one processor is programmed or configured for isolating the at least one image data region within the image data to be obfuscated that comprises the at least one boundary within the at least one image data region that comprises the at least one photo detected within the at least one image data region, or the at least one block of contiguous OCR isolated characters within the image data region, or at least one row comprising at least one block of OCR isolated characters within the image data region, or any combination thereof.

20. The system of claim 11, wherein the at least one processor is programmed or configured to perform image processing operations comprising at least one of the following:

- performing a subsampling operation on the image data;
- performing an image segmentation locating the at least one sensitive datum;
- performing an edge detection operation on the image data containing the at least one sensitive datum;
- performing at least one operation that bounds the at least one sensitive datum;
- performing at least one face detection operation on the image data;
- performing at least one OCR operation on the image data;
- performing at least one blurring operation on the image data containing the at least one sensitive datum;
- performing a at least one masking operation on the image data containing the at least one sensitive datum;
- performing at least one pixelation operation on the image data containing the at least one sensitive datum;
- performing at least one image generation and/or output operation; or any combination thereof.