

CLAIMS

1. An image validation system comprising:
one or more processors; and
memory communicatively coupled to the one or more processors and storing one or more modules that, when executed by the one or more processors, cause the image validation system to perform operations comprising:
obtaining, from a computing device, an image for verification;
in response to obtaining the image, determining the authenticity of the image based on at least two of the following operations:
analyzing the image to detect a change in pixel density from a first portion of the image to a second portion of the image;
comparing the image to a thumbnail of the image to detect a difference between the image and the thumbnail;
analyzing data associated with the image to determine whether image editing software has been used on the image; and
analyzing data associated with the image to identify at least one of a time the image was captured or a geographic location at which the image was captured; and
outputting an indication, based at least in part on the determining the authenticity of the image, of a likelihood that the image has been modified.
2. The image validation system of claim 1, the operations further comprising performing optical character recognition on the image to identify text included in the image; and
wherein the determining the authenticity of the image further includes:
determining that a machine-readable code included in the text of the image is associated with a particular product;
determining that a product key included in the text of the image is in an appropriate format for product keys; and
determining that the product key included in the text of the image includes one or more invalid characters.
3. The image validation system of claim 1 or claim 2, wherein the image comprises a proof of purchase; and wherein the indication of the likelihood that the image has been modified comprises an indication that the image is of a valid proof of purchase.
4. The image validation system of any of claims 1-3, wherein each of the

operations is associated with a weighting factor; and

wherein determining the authenticity of the image further includes:

applying a respective weighting factor to each of the at least two operations to create at least two weighted operations; and

determining the likelihood that the image has been modified based at least in part on the at least two weighted operations.

5. The image validation system of any of claims 1-4, wherein outputting the indication of the likelihood comprises:

determining that the likelihood that the image has been modified is above a first likelihood threshold, below a second likelihood threshold, or between the first likelihood threshold and the second likelihood threshold; and

in response to determining that the likelihood that the image has been modified is above the first likelihood threshold, outputting the indication to the computing device indicating that modification of the image has been detected.

6. The image validation system of any of claims 1-4, wherein outputting the indication of the likelihood comprises:

determining that the likelihood that the image has been modified is above a first likelihood threshold, below a second likelihood threshold, or between the first likelihood threshold and the second likelihood threshold; and

in response to determining that the likelihood that the image has been modified is below the second likelihood threshold, outputting the indication to the computing device indicating that modification of the image has not been detected.

7. The image validation system of any of claims 1-4, wherein outputting the indication of the likelihood comprises:

determining that the likelihood that the image has been modified is above a first likelihood threshold, below a second likelihood threshold, or between the first likelihood threshold and the second likelihood threshold; and

in response to determining that the likelihood that the image has been modified is between the first likelihood threshold and the second likelihood threshold, outputting the indication to the computing device indicating that modification of the image is probable.

8. The image validation system of claim 7, the operations further comprising: sending a request to the computing device for additional information, the additional information comprising at least one of:

an additional image of the subject depicted in the image, the additional

image capturing the object from an angle different than an angle from which the image was captured; or

a video of the object contained in the image.

9. The image validation system of any of claims 1-8, wherein the at least two operations further include:

comparing at least one of:

features of the image to features of a stored image; or

metadata of the image to metadata of the stored image.

10. The image validation system of any of claims 1-9, wherein the likelihood that the image has been modified includes a likelihood that a subject depicted in the image has been modified.

11. A computer-implemented method comprising:

obtaining, via a computing device, an image to be verified;

sending, by the computing device, the image to an image verification service to determine whether the image has been tampered with or not based on a multi-factor analysis;

receiving, at the computing device and from the image verification service, an indication of a likelihood that the image has been tampered with; and

outputting, by the computing device, the indication of the likelihood that the image has been tampered with.

12. The computer-implemented method of claim 11, further comprising:

receiving metadata associated with image and analysis performed by the image verification service; and

causing the image, the likelihood, the metadata, and the analysis to be stored in a data store.

13. The computer-implemented method of claim 11 or claim 12, further comprising:

identifying additional information associated with the image, the additional information including at least one of a device identification (ID) of a consumer computing device associated with the image, an Internet Protocol (IP) address associated with the consumer computing device, or a geographic location associated with the consumer computing device; and

sending the additional information to the image verification service.

14. The computer-implemented method of any of claims 11-13, wherein the

indication of the likelihood that the image has been tampered with comprises an indication that tampering is probable; and wherein the computer-implemented method further comprises outputting, by the computing device, a request for additional information to determine whether the image has been tampered with or not.

15. A computer-implemented method comprising:

obtaining, via a computing device, a digital image for verification;

in response to obtaining the digital image, analyzing the digital image to determine a likelihood that at least one of the digital image or a subject depicted in the digital image has been modified, the analyzing comprising at least two of the following operations:

analyzing the digital image to detect a change in pixel density from a first portion of the digital image to a second portion of the digital image;

comparing the digital image to a thumbnail of the digital image to detect a difference between the digital image and the thumbnail;

analyzing metadata of the digital image to determine whether editing software has been used on the digital image; and

analyzing a comparison between the digital image and a stored digital image to identify similarities between the digital image and the stored digital image; and

outputting an indication, based at least in part on the analyzing the digital image, of the likelihood that at least one of the digital image or the subject depicted in the digital image has been modified.