METHODS AND A COMPUTING DEVICE FOR DETERMINING WHETHER A MARK IS GENUINE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the priority benefit of U.S. Provisional Patent Application 62/307,901, filed on March 14, 2016 and incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure is related generally to anti-counterfeiting technology and, more particularly, to methods and a computing device for determining whether a mark is genuine.

BACKGROUND

[0003] Counterfeit products are, unfortunately, widely available and often hard to spot. When counterfeiters produce fake goods, they typically copy the labeling and bar codes in addition to the actual products. At a superficial level, the labels and bar codes may appear genuine and even yield valid data when scanned (e.g., decode to the appropriate Universal Product Code). While there are many technologies currently available to counter such copying, most of these solutions involve the insertion of various types of codes, patterns, microfibers, microdots, and other indicia to help thwart counterfeiting. Such techniques require manufacturers to use additional equipment and material and add a layer of complexity to the production process.

SUMMARY OF INVENTION

[0003a] According to a first aspect of the present invention, there is provided, on a computing device, a method for determining whether a candidate mark is genuine, the method comprising:

receiving a captured image of a genuine mark;

measuring, using the captured image, a characteristic of the genuine mark at a plurality of locations within the genuine mark, resulting in a set of metrics for the characteristic for the genuine mark;

generating, based on the set of metrics, an electronic signature for the genuine mark;

repeating the receiving, measuring, and generating steps for each of a plurality of genuine marks, resulting in a plurality of genuine signatures;

carrying out a statistical correlation analysis of the plurality of genuine signatures;

determining, based on the statistical correlation analysis, which signatures are sufficiently correlated to indicate that the marks they represent were printed on the same printer;

based on the correlation determination, clustering the genuine signatures of the plurality into a plurality of clusters;

generating a sibling signature for each of the plurality of clusters;

receiving a captured image of a candidate mark;

measuring, using the captured image, a characteristic of the candidate mark at a plurality of locations within the genuine mark, resulting in a set of metrics for the characteristic for the candidate mark;

generating, based on the set of metrics, an electronic signature for the candidate mark;

comparing the electronic signature of the candidate mark with the sibling signature of each of the plurality of clusters to identify which cluster is the best match for the candidate mark;

comparing the electronic signature of the candidate mark to each of the electronic signatures of the cluster identified to be the best match;

determining whether the candidate mark is genuine based the comparison of its electronic signature with each of the electronic signatures of the cluster identified to be the best match; and

generating a message to a user based on the genuineness determination.

[0003b] According to a second aspect of the present invention, there is provided, on a computing device, a method for determining whether a candidate mark is genuine, the method comprising:

receiving a captured image of a genuine mark;

measuring, using the captured image, a characteristic of the genuine mark at a plurality of locations within the genuine mark, resulting in a set of metrics for the characteristic for the genuine mark,

wherein the plurality of locations corresponds to a plurality of location identifiers;

generating, based on the set of metrics, an electronic signature for the genuine mark;

repeating the receiving, measuring, and generating steps for each of a plurality of genuine marks, resulting in a plurality of genuine signatures;

determining, based on a statistical correlation analysis of the plurality of genuine signatures, which genuine signatures are sufficiently correlated to indicate that the marks they represent were printed on the same printer;

based on the statistical correlation analysis, clustering the genuine signatures of the plurality into a plurality of clusters;

generating a sibling signature for each of the plurality of clusters;

deriving a hash identifier for the sibling signature using a subset of the plurality of location identifiers;

receiving a captured image of a candidate mark;

measuring, using the captured image, a characteristic of the candidate mark at a plurality of locations within the candidate mark, resulting in a set of metrics for the characteristic for the candidate mark;

generating, based on the set of metrics, an electronic signature for the candidate mark;

deriving a hash identifier for the electronic signature of the candidate mark using a subset of the plurality of location identifiers;

comparing the hash identifier of the candidate mark with the hash identifier of each of the plurality of clusters to identify which cluster is the best match;

comparing the electronic signature of the candidate mark to each of the electronic signatures of the cluster identified to be the best match;

determining whether the candidate mark is genuine based the comparison of its electronic signature with each of the electronic signatures of the cluster identified to be the best match; and

generating a message to a user based on the determination.

[0003c] According to a third aspect of the present invention, there is provided a computing device that carries out actions comprising:

receiving a captured image of a genuine mark;

measuring, using the captured image of the genuine mark, a characteristic of the genuine mark at a plurality of locations within the genuine mark, resulting in a set of metrics for the characteristic for the genuine mark;

generating, based on the set of metrics for the genuine mark, an electronic signature for the genuine mark;

repeating the receiving, measuring, and generating steps for each of a plurality of genuine marks, resulting in a plurality of genuine signatures;

carrying out a statistical correlation analysis of the plurality of genuine signatures;

determining, based on the statistical correlation analysis, which signatures are sufficiently correlated to indicate that the marks they represent were printed on the same printer;

based on the correlation determination, clustering the genuine signatures of the plurality into a plurality of clusters;

generating a sibling signature for each of the plurality of clusters;

receiving a captured image of a candidate mark;

using the captured image of the candidate mark, measuring the characteristic at a plurality of locations within the candidate mark, resulting in a set of metrics for the characteristic for the candidate mark;

generating, based on the set of metrics for the candidate mark, an electronic signature for the candidate mark;

comparing the electronic signature of the candidate mark with the sibling signature of each of the plurality of clusters to identify which cluster is the best match for the candidate mark;

comparing the electronic signature of the candidate mark to each of the electronic signatures of the cluster identified to be the best match;

determining whether the candidate mark is genuine based the comparison of its electronic signature with each of the electronic signatures of the cluster identified to be the best match; and

generating a message to a user based on the genuineness determination.

DRAWINGS

[0004] While the appended claims set forth the features of the present techniques with particularity, these techniques, together with their objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

[0005] FIG. 1 is an example of a system in which various embodiments of the disclosure may be implemented.