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

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of U.S. Patent Application 14/623,925, filed February 17, 2015 (now U.S. Patent No. 9,519,942) the contents of which are 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 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,

wherein the plurality of locations is associated with a plurality of location identifiers;

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

extracting a waveform from the set of metrics, wherein the waveform is based on an ordered pair relationship between the set of metrics and the plurality of locations;

dividing the waveform into a plurality of bands;

for each band of the plurality of bands,

extracting an attribute of the band;

assigning a numerical value based on the attribute, resulting in a set of numerical values;

forming a hash identifier for the genuine mark from the set of numerical values;

storing the hash identifier in a database in association with the electronic signature of the genuine mark, wherein the database

includes a plurality of electronic signatures of genuine marks and a plurality of hash identifiers, each electronic signature being associated with its own hash identifier, and

is maintained on one or more media storage devices;

receiving a request to determine whether a candidate mark is genuine; and

comparing a hash identifier of the candidate mark with one or more of the plurality of hash identifiers in the database in order to locate at least one possibly-matching electronic signature of a genuine mark.

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

receiving a captured image of a candidate mark;

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

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

wherein the plurality of locations is associated with a plurality of location identifiers,

generating, based on the first set of metrics and the second set of metrics, an electronic signature for the candidate mark,

wherein a first waveform represents an ordered pair relationship between the first set of metrics and the plurality of locations and a second waveform represents an ordered pair relationship between the second set of metrics and the plurality of locations;

filtering the second waveform and the second waveform;

dividing the first filtered waveform into a first plurality of bands;

to each band of the first plurality of bands, assigning a numerical value based on an attribute of the first filtered waveform within the band, resulting in a second set of numerical values;

dividing the second waveform into a second plurality of bands;

to each band of the second plurality of bands, assigning a numerical value based on an attribute of the second filtered waveform within the band, resulting in a second set of numerical values;

forming a hash identifier for the candidate mark using the first set of numerical values and the second set of numerical values;

determining, based on a comparison of the hash identifier of the candidate mark with a hash identifier of a genuine mark, whether the hash identifier of the candidate mark closely matches the hash identifier of the genuine mark;

if the hash identifier of the candidate mark is determined to closely match the hash identifier of the genuine mark, then

retrieving, from a media storage device, an electronic signature of the genuine mark, wherein the electronic signature of the genuine mark contains data regarding an artifact of the genuine mark; and

determining, based on a comparison of the electronic signature of the candidate mark with the retrieved electronic signature of the genuine mark, whether the candidate mark is genuine;

if the candidate mark is determined to be genuine, then indicating that the candidate mark is genuine.

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

receiving a captured image of a genuine mark;

generating an electronic signature for the genuine mark by carrying out steps comprising:

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

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

wherein the plurality of locations is associated with a plurality of location identifiers;

forming the electronic signature for the genuine mark based on the first set and second set of metrics;

generating a hash identifier for the genuine mark by carrying out steps comprising:

extracting a first waveform from the first set of metrics, wherein the first waveform is based on an ordered pair relationship between the first set of metrics and the plurality of locations;

applying a moving average to the first waveform to derive a first filtered waveform;

extracting attributes of the first filtered waveform;

extracting a second waveform from the second set of metrics, wherein the second waveform is based on an ordered pair relationship between the second set of metrics and the plurality of locations;

applying a moving average to the second waveform to derive a second filtered waveform;

extracting attributes of the second filtered waveform;

forming the hash identifier for the genuine mark from the attributes of the first filtered waveform and the attributes of the second filtered waveform;

storing the hash identifier in a database in association with the electronic signature of the genuine mark,

wherein the database

includes a plurality of other electronic signatures and a plurality of other hash identifiers, each electronic signature being associated with its own hash identifier, and

is maintained on one or more media storage devices;

receiving, from a requestor, a captured image of a candidate mark with a request to determine whether the candidate mark is genuine;

generating an electronic signature for the candidate mark by carrying out steps comprising:

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

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

forming the electronic signature for the candidate mark based on the first set and second set of metrics;

generating a hash identifier for the candidate mark by carrying out steps comprising:

extracting a first waveform from the first set of metrics of the candidate mark, wherein the first waveform is based on an ordered pair relationship between the first set of metrics of the candidate mark and the plurality of locations;

applying a moving average to the first waveform to derive a first filtered waveform for the candidate mark;

extracting attributes of the first filtered waveform;

extracting a second waveform from the second set of metrics of the candidate mark, wherein the second waveform is based on an ordered pair relationship between the second set of metrics of the candidate mark and the plurality of locations;

applying a moving average to the second waveform of the candidate mark to derive a second filtered waveform for the candidate mark;

extracting attributes of the second filtered waveform of the candidate mark;

forming the hash identifier for the candidate mark from the measured attributes of the candidate mark's first filtered waveform and the measured attributes the candidate mark's second filtered waveform;

determining, based on a comparison of the hash identifier of the candidate mark with the hash identifier of the genuine mark, whether the hash identifier of the candidate mark closely matches the hash identifier of the genuine mark;

if the hash identifier of the candidate mark is determined to closely match the hash identifier of the genuine mark, then

retrieving, from a media storage device, the electronic signature of the genuine mark; and

determining, based on a comparison of the electronic signature of the candidate mark with the retrieved electronic signature of the genuine mark, whether the candidate mark is genuine;

if the candidate mark is determined to be genuine, then transmitting a message to the requestor indicating that the mark is determined to be genuine.

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;