

That is, the small squares will never fill the template (sized for the middle square) so there will not be a dot. When the template finds the large squares, there will be more than one match where the template is fully white so a series of contiguous dots or a large dot will be the result. The large squares will also then be disqualified.

[0123] Other techniques may be employed to compliment the hit-or-miss transform. For example, statistical analyses may be employed to account for the effects of mis-alignment or other problems. Multiple scans may further be employed to increase the versatility of the hit-or miss transform.

[0124] Selection of a particular morphology determining algorithm, or combination of algorithms, depends on various factors, such as the nature of the security feature intended for detection. Morphological determining algorithms are also referred to herein as “shape determining algorithms.” However, referring to such an algorithm as a “shape determining” algorithm is not meant to be limiting the algorithm to determination of shape, other features (e.g., size) may be determined by the algorithm.

[0125] In preferred embodiments, once a determination has been made that a particle is an authentic security particle **1150** (i.e., at least that it has a valid color and a valid geometric aspect), the position of the particle within the image **404** is recorded. The CMS **15A** then resumes searching for additional particles **1150**. Since the position of the security particle **1150** is known, it can be considered that the region of pixels representing the authentic security particle **1150** is essentially “erased” from the image **404**, and need not be examined again.

[0126] Counting pixels **1110** is one embodiment of a morphological determining algorithm, and is not limiting of the invention disclosed herein. Embodiments of counting pixels **1110** and other morphological (or shape) determining algorithms, may require certain initial conditions. For example, knowledge of the dimensions of the substrate **200** may be required, in order to ascertain dimensions of security features. Alternatively, the geometry of the substrate **200** in relation to the device **5** may be required to provide for derivation of the size of the appearance of the security particles **1150**.

[0127] Counting pixels may be used in some embodiments of a morphological determining algorithm to ascertain the presence of a certain shape. For example, the morphological determining algorithm may identify that one portion of the perimeter of a security particle **1150** runs substantially parallel to another portion of the perimeter of the security particle **1150**, the result being indicative of a fiber **1260** or other elongated structure. Accordingly, it can be considered that executing a morphological determining algorithm provides for determining a “geometric aspect” (or a “morphological aspect”) of the security particle **1150**. As counting proceeds along the perimeter, directional data can be incorporated. That is, identification that one aspect of the perimeter of a security particle **1150** (e.g., an edge) bears a certain relation to another aspect of the security particle **1150** (e.g., is parallel to another edge) may make use of a direction indicated by following a portion of the perimeter of the security particle **1150**.

[0128] FIG. 10A depicts aspects of further embodiments of a perimeter walk. In FIG. 10A a fiber **1260** is shown as

a security feature that is in addition to the security particles **1150**. As an example of a perimeter walk about the fiber **1260**, the CMS **15A** traces the perimeter **1265**, starting at one end of the fiber. The CMS **15A** counts the pixels **1110** as described above, also making record of the direction. That is, the CMS **15A** records that the perimeter **1265** extend in a linear direction, about seven pixels **1110** in distance, along at least one side. Accordingly, the CMS **15A** determines that the security feature is a fiber **1260**, and proceeds with appropriate qualification for authentication.

[0129] Preferably, counting pixels **1110** and other morphological determining algorithms are appropriately designed to account for phenomena that may occur in the detection of a given security feature. For example, it is known that edge effects play a role in the detection of very small security features. As used herein, “edge effects” refers to blending, scatter, and other phenomena that may lead to detection problems. Edge effects can be qualified by statistical methods, or combinations which rely on other security features more easily detected for a significant portion of the authentication algorithm, while the security features characterized by having edge effects play a lesser role.

[0130] Another verification step may involve code qualification. A number of embodiments of coding are possible. That is, codes may be assembled using mixes of colors, by controlling loading, by controlling size, and/or other aspects of a security particle **1150**. As a rudimentary example, one code uses three colors that are a certain mixture of blue, green and yellow. In this embodiment, code verification involves a “count up” approach, where the number of genuine color determinations for each color, such as yellow, is tracked. Once a specific number of positive comparison tests have occurred, the color yellow is certified as being present. The same process is completed for the other colors. Once all colors (blue, green and yellow) are certified as being present, the code is validated and authentication is considered successful.

[0131] Further aspects of qualification of the same code structure relate to detection of counterfeit documents **200**. For example, finding a number of security features having colors that lie close to, but outside of, a respective color cone may be tracked as well. Should a sufficient number of outlying data points be present, the certain color may be decertified and the user may be informed the document **200** is a suspect document **200**.

[0132] Two important considerations lie in use of count up algorithms for code qualification. First, the number of genuine counts needed to certify a color is preferably set low enough to pass detection and measurement requirements, while avoiding false-positive detections. Secondly, the loading of substrate **200** with security features **1150** is preferably high enough to statistically exceed random count results, while being acceptable for field use.

[0133] Therefore, certain thresholds may be established to provide assurance against false positive detection. For example, a given color code may be rejected in five or more instances of a color code that is near to, but outside of, a color cone. Exemplary color codes include, and are not limited to, BGY, GY, Y, G, BGW, BW, GW, W, GYW, and YW, where B=blue, Y=yellow, W=white, and G=green.

[0134] It should be recognized that this is but one embodiment of a code, and the code qualification. Many other