

FIG. 2C—with the distances D1,D2,D3 encountered sequentially when the potential mark constituents PMC are examined in a clockwise order. In an alternative embodiment, each potential security mark PSM is matched against a series of security mark templates, wherein the templates are devised so that, if the potential security mark represents an actual security mark, one template will be matched regardless of any rotational shift of the constituents of the potential security mark—i.e., the entire potential security mark will be compared to a template of an actual security mark, wherein the templates encompass every possible rotational arrangement in which the constituents of the potential security mark could define an actual security mark.

If a neighborhood does not satisfy the sub-step S4b-2, the sub-step S4a-3 bypasses the potential mark constituent PMC about which the neighborhood is established and another potential mark constituent PMC is processed beginning with the sub-step S4a-1. On the other hand, if a neighborhood satisfies the sub-step S4b-2, the sub-step S4c identifies the neighborhood as a potential security mark PSM (FIG. 7B), and processing in accordance with the macro-detection operation S4 continues at S4a-1 for the next potential mark constituent PMC not already part of a potential security mark PSM.

If the macro-detection operation S4 results in the identification of any potential security marks PSM, processing continues with a verification operation S5 in accordance with the present invention as illustrated in FIG. 8. Because the binarization S2, micro-detection S3, and macro-detection S4 operations all preferably rely upon “ranges” or otherwise allow some variation in connection with the identification of potential mark constituents and potential security marks in terms of color, size, shape, and the like, it is possible that one or more of the potential mark constituents PMC defining a potential security mark PSM are not actual mark constituents MC. Of course, in such case, the potential security mark PSM would not be an actual security mark SM. Thus, to ensure that a potential security mark PSM is an actual security mark SM, the potential security mark is subjected to a verification operation S5 in accordance with the present invention. More particularly, for each potential security mark PSM, a verification sub-step S5a-1 examines the color of each potential mark constituent PMC defining the potential security mark PSM, and determines if the color of each potential mark constituent is sufficiently close to or uniform with the color of the other potential mark constituents PMC defining the potential security mark PSM. It is preferred that the potential mark constituents have a color that is equal or close to each other. For example, if two potential mark constituents PMC have respective colors that fall within the color range used in the binarization color-checking sub-step S2a, but the respective colors thereof are found at extreme opposite ends of the acceptable color range, such potential mark constituents will not be deemed to exhibit sufficient color uniformity relative to each other to be actual mark constituents MC. Any potential security marks PSM not satisfying the color uniformity verification sub-step S5a-1 are discarded by the sub-step S5c.

For potential security marks PSM satisfying the color uniformity verification sub-step S5a-1, a dimensional uniformity verification sub-step S5a-2 examines the potential mark constituents PMC for dimensional uniformity relative to each other. The dimensional uniformity verification sub-step S5a-2 examines the column width and/or row height of each potential mark constituent PMC defining the potential security mark PSM for purposes of ensuring that the dimensions of the potential mark constituents are consistent rela-

tive to each other. Again, for example, if one potential mark constituent PMC exhibits dimensional characteristics relative to other potential mark constituents that vary by +/-5%, the potential mark constituent will fail the dimensional uniformity verification sub-step S5a-2, and the sub-step S5c will discard the relevant potential security mark PSM. If the potential mark constituents PMC defining a potential security mark PSM satisfy the verification operation S5, a sub-step S5B identifies the potential security mark PSM as an actual security mark SM.

Subsequent to the verification operation S5, a prevention operation S6 operates to prevent effective reproduction of the document scanned by the image input scanner 12.

A sub-step S6a determines if an actual security mark SM has been identified as present in the document being scanned by the input scanner 12. If no security mark SM has been found, reproduction of the document is permitted. If, on the other hand, a security mark SM is identified, a prevention sub-step S6b prevents effective duplication of the document scanned by the input scanner 12. This is accomplished using one or more suitable prevention operations such as disabling the image output device 16, not sending output data from the image processing unit 14 to the image output device 16, embedding or otherwise including a message (such as VOID) in the image data sent to the image output device 16 so that the message is visible in the document reproduction, or by any other suitable method that prevents an effective reproduction of the document scanned by the input scanner 12.

The invention has been described with reference to preferred embodiments. Modifications and alterations will occur to others upon reading and understanding the preceding specification. It is intended that the invention be construed as including all such modifications and alterations insofar as they fall within the scope of the appended claims or equivalents thereof.

Having thus described the preferred embodiments, what is claimed is:

1. A method for determining whether an image area contains a security mark, comprising:
  - scanning the image area to produce original pixels in L,a,b color space;
  - filtering the b-component of the scanned image area to attenuate any overlaid lines and to produce smoothed b pixels by computing an average b pixel value;
  - determining a maximum pixel density and a minimum pixel density of the smoothed b pixels in the scanned image area; and
  - calculating the difference between the maximum pixel density and the minimum pixel density, wherein if the difference is greater than a threshold value, a security mark may be present in the image area;
 wherein the average b pixel value is computed in a x by y pixel sub-area of the scanned image area according to the relationship:

$$b_{ij}(avg) = \frac{1}{4}(b_{i-1,j} + b_{i+1,j} + b_{i,j-1} + b_{i,j+1}),$$

where  $b_{ij}(avg)$  is the smoothed b(avg) component of the  $i$ th scan line and  $j$ th pixel.

2. The method of claim 1, wherein the maximum pixel density and minimum pixel density are determined over an  $n \times m$  sub-area of the scanned image area.

3. The method of claim 2, wherein the x by y pixel area is  $2 \times 2$  and the  $n \times m$  sub-area is  $8 \times 8$ .