

using a significant portion of the ink required to render a banknote, the modulation function switches again, and causes a lighter than requested green to be returned. This can be repeated, with a period of  $P$  as shown in the "Square wave" modulation function **620**.

The net effect of using this modulation function is that distinct bands will appear when an image of a banknote is printed. FIG. 7 is a diagram illustrating a document having a modulated color according to an embodiment of the present invention. This is shown in FIG. 7 wherein the finely shaded regions (e.g., **710**) correspond to un-modulated regions in document **700** and the coarsely shaded regions (e.g., **720**) correspond to regions that have had their color modulated. Note that visible marks may appear on the page independently of the orientation of the counterfeit notes.

Although a square wave modulation is shown in FIG. 7, other modulation schemes are possible. For example, the function could be a step, a ramp, a saw tooth, or sinusoidal. An advantage of a square wave is that there is no need to calculate a new modulation for each pixel. One merely changes the look-up table value each time the counter reaches a particular number. Furthermore, in regions where there are a lot of pixels having the characteristic color, the transition from one modulation value to another will be very noticeable. This will make it easy to identify counterfeit notes.

Furthermore, although the banknote is printed in a single color, when a banknote is scanned there will actually be a range of colors. This because each pixel of the scanner falls either completely over the background yellow color, completely on the foreground green, or is divided between the two. If the pixel is divided between the two, the color should be a linear combination of those two colors. In addition, as mentioned before, there is the possibility that instead of printing on white paper, a counterfeiter would print on yellow paper and would then alter the scanned note to make all colors a combination of white and green, rather than yellow and green. Both of these possibilities can be programmed into the suspicious region of the LUT space.

Note that should a counterfeiter print more than one banknote on the same page, the visible stripes will appear on all of the notes, although the frequency may increase with the number of notes.

Furthermore, if modulation of the look-up table is performed (for example, instead of denial of printer), the detection need not be perfect. If we consider a general image with a lot of green, we notice that the effect of the method is minimal. The reason the modulated colors of a general image are generally not visible is that although many pixels meet the criterion of being classified as "banknote green" in the LUT, they are dispersed and a minor increase or decrease in the value is not as noticeable as when a large amount of that ink is used in close proximity, as is the case on the back of a banknote.

It may be desirable to enhance the first level detection mechanism. For example as mentioned before, in the case of multi-color secure documents, although use of any of the programmed colors is not considered suspicious, collective use of above-threshold amounts of all, or most of them, is suspicious. Thus, independent events that occur with low probability and which are not in themselves suspicious (in this case the use of more than a threshold amount of a single particular color), can be used to trigger suspicion when a number of the events occur together.

We can also use color detection in combination with detection of geometric features. For example, a secure document can be designed with a geometric feature printed

in an uncommon color. Once a certain amount of this color is detected, a local check for that feature or series of features can be carried out.

It should be clear that one could use various different actions when a suspicious event is found. One could refuse all further function by stopping the rendering process. In certain cases it may be desirable to deteriorate selectively the rendering, once the first level detection has classified a document as suspicious. This could occur in addition to, or instead, of the second level detection mechanism. Preferably, deterioration should affect aspects of the printer's capability that matter more for counterfeit copies than for legitimate documents. These include individual or combinations of the following:

Deliberate mis-rendering of color. Once a threshold amount of a suspicious color is detected, this color can be mis-rendered by modulating the color with a function of the amount used.

Deliberate mis-registration. Addition of a small, unpredictable jitter to the coordinates on the physical page from which rendering begins will make accurate registration between sides of the page extremely difficult.

Deliberate deterioration of halftoning. Substitution of a poorer quality dither matrix, or substitution of non-optimized weight for error diffusion will make reproduction of accurate detail more difficult.

To summarize, the present invention has the following advantages:

It causes negligible impact on time to render a page.  
It has negligible effect on general images and documents, while generating visible artifacts on banknote images or denying their printing.

It can be deployed in the driver with no hardware changes.  
The modulation function can be changed or fine-tuned; e.g.  $T$ ,  $\delta$  and  $P$  in the example we have shown can be adjusted.

The area of the LUT that is classified as suspicious can be adjusted to arrive at a compromise that allows reasonable detection, while giving minimal effect on legitimate users.

No redesign or reissue of currency is required. This method helps detect the existing currency circulation.

Furthermore, so long as the characteristic color does not change, no alteration is required for a new series of notes.

The many features and advantages of the invention are apparent from the written description and thus it is intended by the appended claims to cover all such features and advantages of the invention. Further, because numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

What is claimed is:

1. A method of deterring counterfeit reproductions of a document image, comprising the steps of:

a) counting a number of document image pixels having a characteristic color within a pre-determined color range defined by a lookup table; and

b) performing a color transition frequency test to confirm a counterfeit attempt, if the count exceeds a threshold.

2. The method of claim 1 further comprising the step of:  
c) degrading a reproduction of the document image, if the counterfeit attempt is confirmed.