

choices, while colors that are less common are good candidates. For some documents, detection of several different colors is better than reliance on detection of one color. For example, if each of seven different colors appears in legitimate documents with probability 0.1 (i.e., each color appears on about 10% of documents), appearance individual tokens, or patterns of tokens, of all seven colors would occur in only one legitimate document in ten million (assuming independence).

Detecting the suspicious colors can be performed using in a look-up table (LUT), either specially designed for the purpose, or already in use in the printer, scanner or software pipeline. If the LUT is already part of the pipeline, a parameter can be added to the output of the LUT to indicate when a suspicious region of the LUT input space has been accessed. If more than one color is being detected, one or more parameters can be returned by the LUT to indicate which color was detected. Note that if the LUT is designed only for this detection purpose, these parameters may be the only output of the LUT.

Implementation details of the first and second level detection mechanism will vary depending on the constraints of the device on which it is to be implemented. Color conversion LUTs are commonly smaller than the input space of the image. That is, the LUTs do not contain an entry for every possible input, but have entries for some portion of the possible inputs, and have an interpolation algorithm to expand them. For example although the LUT for a 24-bit RGB image ideally ought to be 256*256*256, a far smaller table, say 30*30*30, will often suffice.

Even so, if memory size is critical, the LUT can consume considerable space. This factor is especially important when designing an ASIC. In such a case, the extra bit (or bits) per entry needed to detect the tokens, might have a non-negligible cost impact on the detector. Because the bits added to the LUT in the first-level detection are not required to reproduce accurate colors, and are used merely to characterize regions of the LUT as being suspicious, it is possible to employ yet a smaller LUT, of size, say 6*6*6, that will be used exclusively for the detection of suspicious regions of color. This additional LUT will take far less memory space than would be needed to combine the color conversion and suspicious color detection functions into one LUT. Accesses to this table could be used before or after the accesses to the main color conversion LUT, or could be accessed in parallel, if the hardware or software architecture permits parallel computation.

Note also that detection of the tokens need not be performed during color look-up, but could be performed at any suitable point in the image pipeline, perhaps even as a preprocessing or postprocessing operation.

Returning to the additional higher level tests, an example of a method suitable for the second level detection is one that detects some visible mark or geometric feature. As pointed out earlier, efficiency of the higher level detection mechanism is no longer as critical, because very few pages will ever be examined by this detector. Any scheme that detects any characteristic feature or series of features on the note will serve. A preferred characteristic of the higher level detection mechanism is that, once the lower-level detection has characterized the page as suspicious, there should still be a sufficient amount of the note remaining to be printed to permit the higher level detection to make an unambiguous decision. However, alternatively, the higher level detection could reprocess an entire document after it had been identified as suspicious.

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 higher 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 detection function can be changed or fine-tuned to trade-off between speed and accuracy.

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.

Only minimal redesign of currency or other secured documents is required.

Furthermore, so long as the characteristic color or pattern 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. An apparatus for deterring counterfeiting of documents, the apparatus comprising:

a first-level detector adapted to detect an initial token having a characteristic color and to thereby quickly eliminate from suspicion a majority of types of the documents without the initial token as legitimate while identifying a minority of types of the documents with the initial token as potentially counterfeit documents;

a second-level detector adapted to further test the potentially counterfeit documents identified by the first-level detector to search for a second token spaced at one of a set of one or more predetermined distances from the initial token, such that detection of the second token can verify which of the potentially counterfeit documents are counterfeit copies; and

an alarm adapted to signal detection of the counterfeit documents by the second-level detector.