

17

18. The machine of claim 17 wherein the symbols comprise a graphic having a length, a width, and blank space.

19. The machine of claim 18 wherein the graphic has an aspect ratio, comprising the length divided by the width, of at least three.

20. The machine of claim 18 wherein the width is less than the length and the length is at least three dots long.

21. The machine of claim 18 further comprising the processor programmed to execute a reading application effective to reading the binary symbols, and wherein the length is sufficiently long to be readable by the reading application, while the length and width are sufficiently small to be unrecognizable to a user.

22. The machine of claim 21 wherein the length and width are sized to be effective to indicate an orientation of the symbols when read by the reading application.

23. A method for providing media-independent security for a document containing security information associated with the document, the method comprising:

inputting, into an input device, image data corresponding to an interpretable image displayable by a display device in an interpretable format to be readily interpretable by a user;

inputting into the input device security data corresponding to the security information;

creating, in a first medium, a document comprising:

a substantive portion containing substantive data corresponding to the image data and transferable in a plurality of media;

a security portion independent from the substantive portion, the security portion comprising symbols unintelligible to a user by visual inspection of the document in the readable format, and the symbols, arranged to represent a security image containing the security data encoded by the symbols, and effective to be inseparably transferred with the document, independent of each medium of the plurality of media, whenever the substantive portion is transferred in said each medium;

transferring the document into a second medium of the plurality of media;

decoding the symbols into binary security data representing the security information; and

outputting the binary security data to an output device in a format retrievable to be interpretable as the security information.

24. the method of claim 23 wherein decoding further comprises:

transforming the symbols in the security portion into a bit map;

capturing a first header containing a target pattern;

synchronizing a reading device to begin reading the symbols proximate the first header;

orienting the reading device in accordance with a direction indicated by the target pattern; and

reading the symbols distributed between the first header and a second header.

25. The method of claim 24 wherein the target pattern is comprised of a selected number of the symbols arranged in a pre-designated pattern.

26. A memory device having blocks of memory effective to store a media-independent security code and an associated document processable by a document processor, the document processor comprising an executable loadable to run on a computer operably associated with the memory device, an input device, and an output device, the memory device comprising:

18

a first block programmed to store an executable, loadable to run on a computer as a document processor application;

a second block programmed to store substantive data corresponding to information in a document presentable in a format interpretable directly by a user;

a third block programmed to store format data useable by the executable to format the substantive data in the document in a layout presentable to the user;

a fourth block programmed to store security data corresponding to security information input through the input device, the security data being independent from the substantive data and stored independently from the substantive data; and

a fifth block programmed to store a security executable, loadable to run on the computer as a security processor effective to process the security data and to include, inseparably from the substantive content, the security data in the document independently of the medium in which the document is represented.

27. The memory device of claim 26 wherein the security executable comprises instructions operable to program the computer to provide output data to the output device effective to produce a security image in the document as output by the output device in a security format rendering the security image uninterpretable by a viewer interpreting the document.

28. The memory device of claim 26 further comprising a rendering buffer storing output data comprising the substantive data and security data combined in a buffer format to be transmitted to the output device.

29. The memory device of claim 28 wherein the buffer format is effective to output to the output device the output data in a transfer format effective to control the output device to output in the document a substantive image corresponding to the substantive data and directly interpretable by a viewer visually inspecting the document, and to output a security image corresponding to the security data and uninterpretable by the viewer.

30. The memory device of claim 28 wherein the rendering buffer stores background data combined with the security data and effective to include the security data in a background image output by the output device in the document.

31. The memory device of claim 28 wherein the rendering buffer stores watermark data combined with the security data and effective to include the security data in a watermark image output by the output device in the document.

32. The memory device of claim 26 further comprising a pattern block comprising pattern encoding data for encoding the security data in a security image to be output in the document by the output device.

33. The memory device of claim 32 wherein the pattern block further comprises palette data corresponding to the pattern encoding data, and effective to present to a user for selection by a user, a plurality of encoding patterns corresponding the encoding data.

34. The memory device of claim 26 wherein the memory device is comprised of a plurality of storage devices adapted to receive data.

35. The memory device of claim 26 further comprising security data corresponding to security codes obscured in a pattern unrecognizable to a user, synchronizing data to synchronize a reader to recognized the pattern, symbol interpretation data to enable the processor to read the pattern to produce a binary code, decoding data to enable the processor to decode the binary code into characters recognizable by a user.