METHOD AND SYSTEM OF EMBEDDING OPTICAL SECURITY FEATURES USING VIRTUAL PRINTER

FIELD OF THE INVENTION

The invention relates generally to a method of intercepting and embedding visible and/or invisible security features into a data stream that is intended for printing.

BACKGROUND

The current approach to printed document security relies primarily on customized applications that use Application Programming Interfaces (API) provided by vendors to embed visible and/or invisible features, herein termed as security features, into the intermediate digital data streams and/or files. The processed data stream(s) and/or file in turn is transmitted to a local or networked printer device for printing.

Due to the need for integration with proprietary APIs into the workflow, digital documents generated by commercial off-the-shelve (COTS) software applications such as word processors and spreadsheets, cannot be easily embedded with such security features prior to printing from printer devices. This also suggests that custom applications developed on top of proprietary optical security feature solutions are coupled at design level and would require implementation changes in the event of migrating to other forms of printed security features. There is a need for a method or a system that alleviates the above problems.

SUMMARY

An aspect of the invention is a method or a system for embedding optical security features in a document comprising providing a computer system having a processor, an application, a virtual printer module, a security feature embedding module and a printer;

receiving data of a digital document to print from the application to the virtual printer module at the printer subsystem; formatting the data with the virtual printer module to a predetermined intermediate format for embedding security features; processing the intermediate formatted data with the security feature embedding module and embedding a predetermined security feature; transmitting the processed data to the printer subsystem via the virtual printer module for printing of the processed data of the digital document.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that embodiments of the invention may be fully and more clearly understood by way of non-limitative examples, the following description is taken in conjunction with the accompanying drawings in which like reference numerals designate similar or corresponding elements, regions and portions, and in which:

FIG. 1 is a block diagram of an embodiment of the invention.

DETAILED DESCRIPTION

In an embodiment of the invention, a way to customize a commercial off-the-shelf (COTS) application of interest is to incorporate the proprietary application programming interface (API) of the selected technology. The feasibility of this approach also depends highly on the design of the application in question and thus may not be an extensible solution. This is especially less feasible and more costly in an enterprise setting where multiple productivity applications are used.

Interaction of COTS application with virtual printer. Referring to FIG. 1, [1] the COTS application will print the digital document of interest using the Virtual printer installed in desktop Operating System (OS) such as Microsoft Windows, Linux and Macintosh. Any OS that has a printer subsystem that communicates to the printer via a software driver

provided the hardware vendor will benefit from this architecture because such printer subsystem typically supports Virtual printer driver. This Virtual printer driver handles all incoming data stream that is submitted to the Virtual printer by any COTS applications that support printing. The suitable OS that has access control mechanisms can be configured to ensure that users can only print via the sanctioned Virtual printer and not to any other printers in the OS running the COTS application.

Formatting of incoming data stream to suitable format for processing. [2] The Virtual printer is capable of communicating with one or more security feature service(s) by means of formatting the incoming data stream from COTS application into a suitable intermediate format such as Postscript, Portable Document Format or any other required format that can be processed by the selected Security feature service(s). The intermediate format of data stream is then communicated to the security feature service(s) by using the relevant proprietary APIs. The communication of this formatted data stream may be via network protocols such as Secure Socket Layer/Transport Layer Security or through any form of inter-process mechanisms

Embedding data stream with optical security features. [3] The security feature service(s) processes the intermediate data stream from the Virtual printer by adding visible and/or invisible optical security features onto the pages represented in the data stream. Typically, the processed data stream is in a format that is readily printable by the hard printer device that could be based on Laser or Inkjet technologies. This processed data stream is transmitted back to the Virtual printer.

Access-controlled redirection of data stream to physical printer. [4] The Virtual printer upon receiving the processed data stream will then redirect the data stream to the actual pre-configured hardware printer device for printing. The OS access control mechanism is configured to permit only print jobs that are initiated from the Virtual printer to the designated hardware printer device. This printer device may be a local or networked device that communicates bi-directionally with the printing subsystem of the OS. The Virtual printer uses the OS standard printing APIs to submit the processed data stream as print job to the printer device via the printing subsystem.

Receiving response from physical printer. [5] Current printer devices are capable of bi-directional communications with the OS printing subsystem. For printers with such capabilities, the Virtual printer is able to perform any form of administrative or auditing tasks (though not limited to), for example to update audit trail upon a response from the hardware printer.

It will be appreciated that embodiments of the invention may provide that any COTS application that supports printing may make use of one or more of such security feature services. Applications are loosely coupled with the security feature services and can migrate or adopt new technologies without further customizations to their COTS or custom applications. Access control of printing resources can be more effectively managed using such an architecture.

While embodiments of the invention have been described and illustrated, it will be understood by those skilled in the technology concerned that many variations or modifications in details of design or construction may be made without departing from the present invention.

CLAIMS:

1. A method for embedding optical security features in a document comprising: providing a computer system having a processor, an application, a virtual printer module, a security feature embedding module and a printer; receiving data of a digital document to print from the application to the virtual printer module at the printer subsystem; formatting the data with the virtual printer module to a predetermined intermediate format for embedding security features; processing the intermediate formatted data with the security feature embedding module and embedding a predetermined security feature; transmitting the processed data to the printer subsystem via the virtual printer module for printing of the processed data of the digital document.