

METHOD AND APPARATUS FOR COPY PROTECTION OF IMAGES IN A COMPUTER SYSTEM

This is a continuation of application Ser. No. 08/289,529
filed on Aug. 12, 1994, now abandoned.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of computer
image display, and in particular, to image protection.

2. Background Art

In the growing multimedia industry, a critical concern to
image creators and image applications developers is image
misappropriation, or piracy. Several pre-existing methods
for protecting images from piracy have been developed,
including watermarks, encryption and proprietary formats.

Watermarks are intentional imperfections in an image
before or after it is converted to digital form. The resultant
lack of quality in the image mitigates the desire to copy the
image. However, watermarking is not satisfactory for imag-
ing and multimedia products as it does not provide the high
image quality required for marketable applications.

A more common method of image protection is encryp-
tion. Image encryption typically involves taking image data
that exists in a standard format, such as GIF or BMP, and
converting it into an unrecognizable data file through the use
of a mathematical encryption algorithm. Prior to display, the
encrypted image is passed through a deciphering process to
regenerate the image data in a displayable format. The
decrypted data is then placed in the video adapter's memory
for use by the display unit.

Without encryption, image files in standard formats are
recognized by a broad range of image processing applica-
tions. For this reason, unencrypted images can be copied and
manipulated through unsanctioned applications. By encrypt-
ing computer files, use of the computer files can be restricted
to only those applications provided with the deciphering
scheme. Image files are therefore substantially protected
from misappropriation up until the moment they are deci-
phered and placed in the video adapter's memory, where a
video adapter is any device connected to the computer's data
bus, including any local bus, that has its own memory or
uses the computer's main memory to render images on a
video display device. Once the image is present in the video
memory in a standard display format, the image is again
susceptible to piracy. Therefore, encryption is a necessary
but incomplete protection scheme.

Proprietary formats are image data formats created for use
in applications unique to the developer. These formats differ
from an encryption scheme in that there often exists a one to
one mapping between the source image file and the stored
image file. Therefore, an expert may be able to recognize the
nature of the data (i.e. that it is image data). In some cases,
it is possible to reverse engineer the proprietary format and
obtain the images. Further, some proprietary formats are
available as part of developer tool kits. The format can be
incorporated into a new application that is able to read or
transfer proprietary image files.

Regardless of what encryption schemes or proprietary
formats are used, an image file must eventually be translated
into a standard image file format when it is supplied to the
memory for the display unit. Once displayed, the image data
sheds all security features. An end user can pirate the image
by copying it from the video adapter's memory and storing

it in any format. The pirated image data can then be
distributed to other destinations.

For example, in the Windows™ operating environment
sold by Microsoft Corporation, a user may pirate an image
by pressing a "PRINT SCREEN" button on a computer
keyboard and storing a bit-mapped image of the screen in a
"clipboard." From the clipboard, the image can be "pasted"
into an image processing application and stored for eventual
unlicensed distribution. Therefore, though current encryp-
tion methods and proprietary formats are useful for securing
image files, they are insufficient for protecting image files
once they are provided to a video adapter's memory.

U.S. Pat. No. 4,241,415 to Masaki et al. discloses an
apparatus for selectively masking portions of visual output.
The apparatus contains a first memory for storing informa-
tion code signals convertible into visible information and a
second memory containing specific code signals in locations
corresponding to the code signals in the first memory which
selectively are not to be visualized. Signals from each
memory are read simultaneously. When the device is in
mask mode and a specific code signal is detected in the
second memory, the corresponding information code signal
in the first memory is masked, either by omission or replace-
ment with a special mark. The Masaki patent does not
suggest use of this apparatus in any security scheme.

U.S. Pat. No. 4,352,100 to O'Connell discloses an image
formatting apparatus for use in changing image contrast or
providing masked borders around selected images. The
apparatus is not designed for security purposes. Further, it
does not act to blank the selected image, but to blank the
areas around it.

U.S. Pat. No. 4,554,584 to Elam et al. discloses an
auxiliary circuit for remote control of television receiver
blanking by digital code words transmitted as part of the
video signal. The circuit allows the end user to determine
what video signals to blank from the display unit.

U.S. Pat. No. 4,881,179 to Vincent discloses a method of
controlling the unauthorized disclosure of classified data in
a calendar application. Only those having a clearance code
equivalent to or higher than the specified clearance code for
the information can receive the calendar information. No
apparatus is disclosed for preventing the copying of calendar
images already present on the screen.

U.S. Pat. No. 4,932,053 to Fruhauf et al. discloses a safety
device for preventing unauthorized detection of protected
data in a memory chip by the use of current sensing
approaches. Random current generators within the chip
produce random current values on output pins of the chip to
conceal actual current values that may indicate memory data
values.

U.S. Pat. No. 5,036,537 to Jeffers et al. discloses a method
for blocking out video signals in a television receiver. No
means are disclosed to prevent copying of images that are
allowed to reach the receiver.

U.S. Pat. No. 5,142,576 to Nadan discloses a key security
system for selectively providing restricted information to
video displays. An encoder transmits display update data
and a key to a plurality of decoders. The decoder that
matches the key receives the update data and places it in the
picture store for a video display. No means are suggested for
preventing the copying of images stored in the picture store
of the video display.

U.S. Pat. No. 5,144,664 to Esserman et al. discloses a
secure communication network serving a plurality of termi-
nals grouped into different security categories. A headend
device has several encryption algorithms stored. In addition,