

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
23 October 2003 (23.10.2003)

PCT

(10) International Publication Number  
**WO 03/088144 A2**

- (51) International Patent Classification<sup>7</sup>: **G06T**
- (21) International Application Number: PCT/US03/11214
- (22) International Filing Date: 9 April 2003 (09.04.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
60/371,335 9 April 2002 (09.04.2002) US  
60/429,115 25 November 2002 (25.11.2002) US
- (71) Applicant (for all designated States except US): **DIGI-MARC ID SYSTEMS, LLC** [US/US]; 19801 SW 72nd Avenue, Suite 250, Tualatin, OR 97062 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **SCHNECK, Nelson** [US/US]; 19 Hardy Lane, Hollis, NH 03049 (US). **DUGGAN, Charles, F.** [US/US]; 8 Derry Street, Merrimack, NH 03054 (US). **JONES, Robert** [US/US]; 1 Coventry Lane, Andover, MA 01810 (US). **BI, Daoshen** [US/US]; 58 Loring Avenue, Boxborough, MA 01719 (US).
- (74) Agent: **MCLAUGHLIN DOWNING, Marianne**; Digimarc ID Systems, LLC, 19801 SW 72nd Avenue, Suite 250, Tualatin, OR 97062 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**  
— without international search report and to be republished upon receipt of that report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*



**WO 03/088144 A2**

(54) Title: IMAGE PROCESSING TECHNIQUES FOR PRINTING IDENTIFICATION CARDS AND DOCUMENTS

(57) Abstract: The invention relates to identification documents, and in particular to preprinting processing covert images, such as UV or IR images, provided on such identification documents. In one implementation, the invention provides a method of processing a digital image that is to be printed on a surface of an identification document as a fluorescing-capable image to improve the quality of the image. Edges or boundaries are detected within the image, the detected edges or boundaries forming an intermediate image. The edges or boundaries within the image are emphasized, and the emphasized image is used for printing the covert image. In some implementations of the invention, a digital watermark is embedded in the covert image.

## IMAGE PROCESSING TECHNIQUES FOR PRINTING IDENTIFICATION CARDS AND DOCUMENTS

### Related Application Data

This application claims the priority of the following United States Provisional

5 Applications:

- Image Processing Techniques for Printing Identification Cards and Documents (Application No. 60/371,335, Attorney Docket No. P0609 -- Inventors: Nelson T. Schneck and Charles Duggan, filed April 9, 2002); and
- 10 • Methods of Providing Optical Variable Device for Identification Documents (Application No. 60/429,115, filed November 25, 2002 – Inventors: Nelson T. Schneck, Charles R. Duggan, Robert Jones, and Daoshen Bi).

This application is also related to the following U.S. patent applications:

- 15 • Use of Pearlescent and Other Pigments to Create Security Documents (Application No. 09/969,020, Attorney Docket No. P0537D, Inventors Bentley Bloomberg and Robert L. Jones, filed October 2, 2001);
- Identification Card Printed With Jet Inks and Systems and Methods of Making Same (Application No. 10/289,962, Attorney Docket No. P0708D, Inventors Robert Jones, Dennis Mailloux, and Daoshen Bi, filed November 20 6, 2002);
- Contact Smart Cards Having a Document Core, Contactless Smart Cards Including Multi-Layered Structure, PET-Based Identification Document, and Methods of Making Same (Application No. 10/329,318, Attorney Docket No. P0711D, filed December 23, 2002--Inventors Robert Jones, Joseph Anderson, Daoshen Bi, Thomas Regan, and Dennis Mailloux,);
- 25 • Ink with Cohesive Failure and Identification Document Including Same (Application No. 10/329,315, Attorney Docket No. P0714D, filed December 23, 2002--Inventors Robert Jones and Bentley Bloomberg);
- 30 • Laser Engraving Methods and Compositions, and Articles Having Laser Engraving Thereon (Application No. 10/326,886, Attorney Docket No. P0724D, filed December 20, 2002—Inventors Brian Labrec and Robert Jones);
- Multiple Image Security Features for Identification Documents and Methods of Making Same (Application No. 10/325,434, Attorney Docket No. P028D, filed December 18, 2002—Inventors Brian Labrec, Joseph Anderson, Robert Jones, and Danielle Batey);
- 35 • Covert Variable Information on Identification Documents and Methods of Making Same (Application No. 10/330032, Attorney Docket No. P0732D, filed December 24, 2002 -- Inventors: Robert Jones and Daoshen Bi);
- 40

- 2 -

- Systems, Compositions, and Methods for Full Color Laser Engraving of ID Documents (Application No. 10/330,034, Attorney Docket No. P0734D, filed December 24, 2002—Inventor Robert Jones); and
- 5     • Laser Etched Security Features for Identification Documents and Methods of Making Same (Application No. 10,330,033, Attorney Docket No. P0736D, filed December 24, 2002—Inventors George Theodossiou and Robert Jones).

The present invention is also related to the following provisional applications:

10

- Identification Document and Related Methods (Application No. 60/421,254, Attorney Docket No. P0703 – Inventors: Geoff Rhoads, et al);
- Identification Document and Related Methods (Application No. 60/418,762, Attorney Docket No. P0696 – Inventors: Geoff Rhoads, et al);
- 15     • Shadow Reduction System and Related Techniques for Digital Image Capture (Application No. 60/410,544, Attorney Docket No. P0689D, filed September 13, 2002 – Inventors: Scott D. Haigh and Tuan A. Hoang).
- Systems and Methods for Recognition of Individuals Using Combination of Biometric Techniques (Application No. 60/418,129, Attorney Docket No. P0698D, filed October 11, 2002 – Inventors James V. Howard and Francis Frazier);
- 20     • Systems and Methods for Managing and Detecting Fraud in Image Databases Used With Identification Documents (Application No. 60/429,501, Attorney Docket No. P0718D, filed November 26, 2003—Inventors James V. Howard and Francis Frazier);
- 25     • Enhanced Shadow Reduction System and Related Technologies for Digital Image Capture (Application No. 60/447,502, Attorney Docket No. P0789D, filed February 13, 2003—Inventors Scott D. Haigh, Tuan A. Hoang, Charles R. Duggan, David Bohaker, and Leo M. Kenen);
- 30     • Integrating and Enhancing Searching of Media Content and Biometric Databases (Application No. 60/451,840, Attorney Docket No. P0803, filed March 3, 2003); and
- Optically Variable Devices with Embedded Data for Authentication of Identity Documents (Application No. not yet assigned, Attorney Docket No. P0816D, filed March 31, 2003—Inventor Robert Jones).
- 35

The present invention is also related to U.S. Patent Application Nos. 09/747,735, filed December 22, 2000, and 09/602,313, filed June 23, 2000, as well as U.S. Patent No. 6,066,594.

40

## Technical Field

The present invention generally relates to identification and security documents, and in particular, relates to enhancing the formation a covert image such as a fluorescing, ultraviolet, infrared, thermachromic and/or optical variable image on such documents.

## Background and Summary

### *Identification Documents*

Identification documents (hereafter "ID documents") play a critical role in today's society. One example of an ID document is an identification card ("ID card"). ID documents are used on a daily basis -- to prove identity, to verify age, to access a secure area, to evidence driving privileges, to cash a check, and so on. Airplane passengers are required to show an ID document during check in, security screening and prior to boarding their flight. In addition, because we live in an ever-evolving cashless society, ID documents are used to make payments, access an automated teller machine (ATM), debit an account, or make a payment, etc.

(For the purposes of this disclosure, ID documents are broadly defined herein, and include, e.g., credit cards, bank cards, phone cards, passports, driver's licenses, network access cards, employee badges, debit cards, security cards, visas, immigration documentation, national ID cards, citizenship cards, social security cards, security badges, certificates, identification cards or documents, voter registration cards, police ID cards, border crossing cards, legal instruments, security clearance badges and cards, gun permits, gift certificates or cards, membership cards or badges, etc., etc. Also, the terms "document," "card," "badge" and "documentation" are used interchangeably throughout this patent application.).

Many types of identification cards and documents, such as driving licenses, national or government identification cards, bank cards, credit cards, controlled access cards and smart cards, carry thereon certain items of information which relate to the identity of the bearer. Examples of such information include name, address, birth date, signature and photographic image; the cards or documents may in addition carry other variant data (i.e., data specific to a particular card or document, for example an employee number) and invariant data (i.e., data common to a large number of cards, for

- 4 -

example the name of an employer). All of the cards described above will hereinafter be generically referred to as "ID documents".

As those skilled in the art know, ID documents such as drivers licenses can contain information such as a photographic image, a bar code (which may contain  
5 information specific to the person whose image appears in the photographic image, and/or information that is the same from ID document to ID document), variable personal information, such as an address, signature, and/or birthdate, biometric information associated with the person whose image appears in the photographic image (e.g., a fingerprint), a magnetic stripe (which, for example, can be on the a side of the  
10 ID document that is opposite the side with the photographic image), and various security features, such as a security pattern (for example, a printed pattern comprising a tightly printed pattern of finely divided printed and unprinted areas in close proximity to each other, such as a fine-line printed security pattern as is used in the printing of banknote paper, stock certificates, and the like).

15 An exemplary ID document can comprise a core layer (which can be pre-printed), such as a light-colored, opaque material (e.g., TESLIN (available from PPG Industries) or polyvinyl chloride (PVC) material). The core is laminated with a transparent material, such as clear PVC to form a so-called "card blank". Information, such as variable personal information (e.g., photographic information), is printed on the  
20 card blank using a method such as Dye Diffusion Thermal Transfer ("D2T2") printing (described further below and also described in commonly assigned United States Patent No. 6066594.) The information can, for example, comprise an indicium or indicia, such as the invariant or nonvarying information common to a large number of identification documents, for example the name and logo of the organization issuing the  
25 documents. The information may be formed by any known process capable of forming the indicium on the specific core material used.

To protect the information that is printed, an additional layer of transparent overlamine can be coupled to the card blank and printed information, as is known by those skilled in the art. Illustrative examples of usable materials for overlaminates  
30 include biaxially oriented polyester or other optically clear durable plastic film.

In the production of images useful in the field of identification documentation, it may be desirable to embody into a document (such as an ID card, drivers license,

- 5 -

passport or the like) data or indicia representative of the document issuer (e.g., an official seal, or the name or mark of a company or educational institution) and data or indicia representative of the document bearer (e.g., a photographic likeness, name or address). Typically, a pattern, logo or other distinctive marking representative of the document issuer will serve as a means of verifying the authenticity, genuineness or valid issuance of the document. A photographic likeness or other data or indicia personal to the bearer will validate the right of access to certain facilities or the prior authorization to engage in commercial transactions and activities.

Identification documents, such as ID cards, having printed background security patterns, designs or logos and identification data personal to the card bearer have been known and are described, for example, in U.S. Pat. No. 3,758,970, issued Sep. 18, 1973 to M. Annenberg; in Great Britain Pat. No. 1,472,581, issued to G. A. O. Gesellschaft Fur Automation Und Organisation mbH, published Mar. 10, 1976; in International Patent Application PCT/GB82/00150, published Nov. 25, 1982 as Publication No. WO 82/04149; in U.S. Pat. No. 4,653,775, issued Mar. 31, 1987 to T. Raphael, et al.; in U.S. Pat. No. 4,738,949, issued Apr. 19, 1988 to G. S. Sethi, et al.; and in U.S. Pat. No. 5,261,987, issued Nov. 16 1993 to J. W. Luening, et al.

#### *Printing Information onto ID Documents*

The advent of commercial apparatus (printers) for producing dye images by thermal transfer has made relatively commonplace the production of color prints from electronic data acquired by a video camera. In general, this is accomplished by the acquisition of digital image information (electronic signals) representative of the red, green and blue content of an original, using color filters or other known means. Devices such as digital cameras, optical sensors, and scanners also can provide digital image information. The digital image information is utilized to print an image onto a data carrier. For example, information can be printed using a printer having a plurality of small heating elements (e.g., pins) for imagewise heating of each of a series of donor sheets (respectively, carrying diffuseable cyan, magenta and yellow dye). The donor sheets are brought into contact with an image-receiving element (which can, for example, be a substrate) which has a layer for receiving the dyes transferred imagewise from the donor sheets. Thermal dye transfer methods as aforesaid are known and

- 6 -

described, for example, in U.S. Pat. No. 4,621,271, issued Nov. 4, 1986 to S. Brownstein and U.S. Pat. No. 5,024,989, issued Jun. 18, 1991 to Y. H. Chiang, et al.

Dye diffusion thermal transfer printing (“D2T2”) and thermal transfer (also referred to as mass transfer printing) are two printing techniques that have been used to print information on identification cards. For example, D2T2 has been used to print images and pictures, and thermal transfer has been used to print text, bar codes, and single color graphics.

D2T2 is a thermal imaging technology that allows for the production of photographic quality images. In D2T2 printing, one or more thermally transferable dyes (e.g., cyan, yellow, and magenta) are transferred from a donor, such as a donor dye sheet or a set of panels (or ribbons) that are coated with a dye (e.g., cyan, magenta, yellow, black, etc.) to a receiver sheet (which could, for example, be part of an ID document) by the localized application of heat or pressure, via a stylus or thermal printhead at a discrete point. When the dyes are transferred to the receiver, the dyes diffuse into the sheet (or ID card substrate), where the dyes will chemically be bound to the substrate or, if provided, to a receptor coating. Typically, printing with successive color panels across the document creates an image in or on the document’s surface. D2T2 can result in a very high printing quality, especially because the energy applied to the thermal printhead can vary to vary the dye density in the image pixels formed on the receiver, to produce a continuous tone image. D2T2 can have an increased cost as compared to other methods, however, because of the special dyes needed and the cost of D2T2 ribbons. Also, the quality of D2T2- printed image may depend at least on an ability of a mechanical printer system to accurately spatially register a printing sequence, e.g., yellow, magenta, cyan, and black.

Another thermal imaging technology is thermal or mass transfer printing. With mass transfer printing, a material to be deposited on a receiver (such as carbon black (referred to by the symbol “K”)) is provided on a mass transfer donor medium. When localized heat is applied to the mass transfer donor medium, a portion (mass) of the material is physically transferred to the receiver, where it sits “on top of” the receiver. For example, mass transfer printing often is used to print text, bar codes, and monochrome images. Resin black mass transfer has been used to print grayscale pictures using a dithered gray scale, although the image can sometimes look coarser

- 7 -

than an image produced using D2T2. However, mass transfer printing can sometimes be faster than D2T2, and faster printing can be desirable in some situations.

Printing of black ("K") can be accomplished using either D2T2 or mass transfer. For example, black monochrome "K" mass transfer ribbons include Kr (which designates a thermal transfer ribbon) and Kd (which designates dye diffusion).

Both D2T2 and thermal ink have been combined in a single ribbon, which is the well-known YMCK (Yellow-Magenta-Cyan-Black) ribbon (the letter "K" is used to designate the color black in the printing industry). Another panel containing a protectant ("P") or laminate (typically a clear panel) also can be added to the YMCK ribbon).

#### *UV Security Features in ID Documents*

One response to the problem of counterfeiting ID documents has involved the integration of verification features that are difficult to copy by hand or by machine, or which are manufactured using secure and/or difficult to obtain materials. One such verification feature is the use in the card of a signature of the card's issuer or bearer. Other verification features have involved, for example, the use of watermarks, biometric information, microprinting, covert materials or media (e.g., ultraviolet (UV) inks, infrared (IR) inks, fluorescent materials, phosphorescent materials), optically varying images, fine line details, validation patterns or marking, and polarizing stripes. These verification features are integrated into an identification card in various ways and they may be visible or invisible (covert) in the finished card. If invisible, they can be detected by viewing the feature under conditions which render it visible. At least some of the verification features discussed above have been employed to help prevent and/or discourage counterfeiting.

Covert security features are those features whose presence is not visible to the user without the use of special tools (e.g., UV or IR lights, digital watermark readers) or knowledge. In many instances, a covert security feature is normally invisible to a user. Some technologies that involve invisible features require the use of specialized equipment, such as a detector or a device capable of reading digital watermarks. One type of covert security feature is the printing of information (images, designs, logos, patterns, text, etc.) in a material that is not visible under normal lighting conditions, but



- 8 -

can be viewed using a special non-visible light source, such as an ultraviolet (UV) or infrared (IR) light source. Use of UV and/or IR security features can be advantageous because although the devices (for example, UV and/or IR light sources) required to see and use such features are commonly available at a reasonable cost, the ability to  
5 manufacture and/or copy at least some implementations of such features is far less common and can be very costly. UV and IR based covert security features thus can help deter counterfeiters because the features cannot be copied by copiers or scanners and are extremely difficult to manufacture without the requisite know-how, equipment, and materials.

10 For example, the assignee of the present invention has developed and marketed a proprietary product called PolaPrime-UV™. PolaPrime-UV™ is a type of security feature. One application of PolaPrime-UV™ is for full color photo quality printing of fixed (i.e., not variable data) fluorescent images. The artwork that can be printed using  
15 PolaPrime-UV™ includes many images that can be produced with a combination of red, green, and blue phosphors. Under the appropriate light (e.g., a light source capable of providing UV light), the effect seen when viewing an image printed with PolaPrime-UV™ is similar in appearance to a television screen in that the image is formed by emission of light rather than reflection as with ink on paper. To date, PolaPrime-UV™ has been a reliable authenticator for genuine identification documents.

20

#### ***Printing of Covert Materials such as UV***

Many images, such as color images, are formed by subtractive techniques, e.g., light is passed through absorbing dyes and the combination of dyes produce an image  
25 by sequentially subtracting cyan, magenta, and yellow components to provide the full color image. In the case of a UV fluorescing image, the UV image is formed by light emitting from fluorescing dyes or pigments as they are activated by a UV light or energy source. A UV image can be imparted to an ID document via methods such as thermal transfer or D2T2.

30 Regardless of whether the UV materials are imparted via D2T2 or mass transfer panel, both panels produce transmissive images – the mass transfer panel produces a bitonal (e.g., two tones) image and the dye sublimation panel produces a monochromatic (or shaded) image.

## Summary

For purposes of identification (e.g., of the bearer of an ID document or of the ID document itself), an ID document includes at least one image that is an “identification quality” likeness of the holder such that someone viewing the card can determine with reasonable confidence whether the holder of the card actually is the person whose image is on the card. “Identification quality” images, in at least one embodiment of the invention, include images that, when viewed using the proper facilitator (e.g., an appropriate light source for certain covert images, an appropriate temperature source for thermachromic images, etc.), provide a discernable image that is usable for identification or authentication purposes. To date, however, it has been very difficult to print images such as driver’s license portraits with covert (i.e., not visible to an unaided human eye) materials/media such as UV, IR, thermachromic (materials whose appearance changes and/or becomes visible to a naked human eye with temperature), ferrofluids (materials whose appearance changes and/or becomes visible to a naked human eye upon application of a magnetic field) materials, where the quality of the covert image is sufficient to enable the image to be relied upon for identification or authentication. This can be especially difficult when attempting to print color images using covert materials.

Further, because of the enhanced security provided by the use of full color UV printing, such as is proposed in co-pending and commonly assigned United States Patent Application No. 10/330,032 (entitled “Covert Variable Information on Identification Documents and Methods of Making Same”), it would be advantageous to be able to print variable or personal UV information at the time of card personalization, in one, two, or three UV colors, especially images that have a high enough quality to be used for authentication and/or identification. It also would be advantageous if the same information could be printed in a visible and invisible (e.g., UV) form at substantially the same time or at substantially the same printing step, where the covert image would be “identification quality”.

In one embodiment of the invention, we provide methods by which one improves a digital image from which a covert image is formed. One aspect of our invention provides improvements to reduce a “washed-out” effect that can occur when a covert image that has been printed using a covert media such as UV ink, IR ink,

- 10 -

thermochromic ink, inks comprising ferrofluids, and the like, is appropriately stimulated so as to cause the covert image to become visible. For example, such washed out effect can be seen when a UV or IR image fluoresces.

One problem that has prevented covert images such as UV or IR images from being “identification quality” is the problem of blurred image details. For example, a problem that can be associated with printing a UV covert image is that since the UV covert image 14 “glows” under appropriate UV stimulation, image details can be less apparent, blurred or can be completely lost. The UV glowing is capable of essentially “washing out” an image’s perceptible crispness (e.g., similar to a situation in which a dimly lighted object is in proximity to a brightly lighted object). Similar problems can exist with IR glowing and with thermochromic inks. The inventors of the instant invention have found that image details can be enhanced to overcome this washout problem. In particular, in at least one embodiment of the invention, the inventors have found that it is possible to digitally process an image prior to printing to compensate for the glowing effect.

UV (and/or IR) image glow which washes out the details of a fluorescing UV (and/or IR) image can thus present a considerable problem in relying upon such covert images for identification. To create a discernable fluorescing image on an ID document (useful for identification and security checks), in accordance with one embodiment of the invention, the inventors have found that we can enhance the digital data that is used to create the UV image. Without the inventive enhancements described herein, for example if one simply prints the digital information as such from a digital camera or scanned image, etc., then one may get gets (when fluorescing) an image that may not as useful for security or identification purposes due to the washed out effect of the UV image. The details of our inventive techniques follow.

In a further embodiment of the invention, steganographic embedded code, such a digital watermark, can be provided in the covert image 14.

In one embodiment, the invention provides a method of processing a digital image that is to be printed on a surface of an identification document as covert image. At least one of edges and boundaries within the image is detected, the detected edges or boundaries forming an intermediate image. The edges or boundaries within the intermediate image are emphasized.

- 11 -

In one embodiment, the invention provides a method of providing a covert image to an identification document. Contrast is increased in at least a portion of the digital image. The contrast-increased portion of the digital image is dithered. The dithered image is transferred to the identification document.

5 In one embodiment, the invention provides an identification document comprising a core layer and a cover image printed to the core layer. The core layer comprises a core material capable of having printed thereon an image formed using a covert medium. The cover image is formed by providing a digital image that is to be used as a model to generate the covert image, increasing the contrast in the digital  
10 image, detecting edges or boundaries within the digital image, the detected edges or boundaries forming an intermediate image, emphasizing the edges or boundaries within the intermediate image, and printing the emphasized intermediate image in a covert medium on the core layer.

The foregoing and other features and advantages of the present invention will be  
15 even more readily apparent from the following Detailed Description, which proceeds with reference to the accompanying drawings and the claims.

### Brief Description of the Drawings

The advantages, features, and aspects of embodiments of the invention will be more fully understood in conjunction with the following detailed description and  
20 accompanying drawings, wherein:

FIG. 1 is an illustration of an identification document in accordance with a first embodiment of the invention;

FIG. 2 is a flow diagram outlining a first aspect of the invention;

FIG. 3 is a flow diagram outlining a second aspect of the invention;

25 FIG. 4 is a flow diagram outlining a third aspect of the invention;

FIGS. 5a-5g are exemplary images illustrating an inventive aspect of the present invention) (FIGS. 5a-5e are provided as black and white photographic images) and in particular:

FIG. 5a is a photographic color image including a headshot of a human subject;

30 FIG. 5b illustrates the image of FIG. 5a with its contrast improved;

FIG. 5c emphasizes the horizontal edges of the FIG. 5b image;

- 12 -

FIG. 5d emphasizes the vertical edges of the FIG. 5b image;  
FIG. 5e illustrates a composite image of FIGS. 5c and 5d;  
FIG. 5f illustrates a binaryized version of FIG. 5e; and  
FIG. 5g illustrates an inverted version of FIG. 5f.

5

Of course, the drawings are not necessarily drawn to scale, with emphasis rather being placed upon illustrating the principles of the invention. In the drawings, like reference numbers indicate like elements or steps.

10

## Detailed Description

### *Terminology*

In the foregoing discussion, the use of the word "ID document" is broadly defined and intended to include all types of ID documents, including (but not limited to), documents, magnetic disks, credit cards, bank cards, phone cards, stored value  
15 cards, prepaid cards, smart cards (e.g., cards that include one more semiconductor chips, such as memory devices, microprocessors, and microcontrollers), contact cards, contactless cards, proximity cards (e.g., radio frequency (RFID) cards), passports, driver's licenses, network access cards, employee badges, debit cards, security cards, visas, immigration documentation, national ID cards, citizenship cards, social security  
20 cards, security badges, certificates, identification cards or documents, voter registration and/or identification cards, police ID cards, border crossing cards, security clearance badges and cards, legal instruments, gun permits, badges, gift certificates or cards, membership cards or badges, and tags. Also, the terms "document," "card," "badge" and "documentation" are used interchangeably throughout this patent application.). In  
25 at least some aspects of the invention, ID document can include any item of value (e.g., currency, bank notes, and checks) where authenticity of the item is important and/or where counterfeiting or fraud is an issue.

In addition, in the foregoing discussion, "identification" at least refers to the use of an ID document to provide identification and/or authentication of a user and/or the  
30 ID document itself. For example, in a conventional driver's license, one or more

- 13 -

5 portrait images on the card are intended to show a likeness of the authorized holder of the card. For purposes of identification, at least one portrait on the card (regardless of whether or not the portrait is visible to a human eye without appropriate stimulation) preferably shows an “identification quality” likeness of the holder such that someone viewing the card can determine with reasonable confidence whether the holder of the card actually is the person whose image is on the card. “Identification quality” images, in at least one embodiment of the invention, include covert images that, when viewed using the proper facilitator (e.g., an appropriate light or temperature source), provide a discernable image that is usable for identification or authentication purposes.

10 There are a number of reasons why an image or information on an ID document might not qualify as an “identification quality” image. Images that are not “identification quality” may be too faint, blurry, coarse, small, etc., to be able to be discernable enough to serve an identification purpose. An image that might not be sufficient as an “identification quality” image, at least in some environments, could, for example, be an image that consists of a mere silhouette of a person, or an outline that does not reveal what might be considered essential identification essential (e.g. hair or eye color) of an individual.

Of course, it is appreciated that certain images may be considered to be “identification quality” if the images are machine readable or recognizable, even if such images do not appear to be “identification quality” to a human eye, whether or not the human eye is assisted by a particular piece of equipment, such as a special light source. For example, in at least one embodiment of the invention, an image or data on an ID document can be considered to be “identification quality” if it has embedded in it machine-readable information (such as digital watermarks or steganographic information) that also facilitate identification and/or authentication.

25 Further, in at least some embodiments, “identification” and “authentication” are intended to include (in addition to the conventional meanings of these words), functions such as recognition, information, decoration, and any other purpose for which an indicia can be placed upon an article in the article’s raw, partially prepared, or final state. Also, instead of ID documents, the inventive techniques can be employed with product tags, product packaging, business cards, bags, charts, maps, labels, etc., etc., particularly those items including marking of an laminate or over-laminate structure.

- 14 -

The term ID document thus is broadly defined herein to include these tags, labels, packaging, cards, etc.

“Personalization”, “Personalized data” and “variable” data are used interchangeably herein, and refer at least to data, images, and information that are  
5 “personal to” or “specific to” a specific cardholder or group of cardholders. Personalized data can include data that is unique to a specific cardholder (such as biometric information, image information, serial numbers, Social Security Numbers, privileges a cardholder may have, etc.), but is not limited to unique data. Personalized data can include some data, such as birthdate, height, weight, eye color, address, etc.,  
10 that are personal to a specific cardholder but not necessarily unique to that cardholder (for example, other cardholders might share the same personal data, such as birthdate). In at least some embodiments of the invention, personal/variable data can include some fixed data, as well. For example, in at least some embodiments, personalized data refers to any data that is not pre-printed onto an ID document in advance, so such  
15 personalized data can include both data that is cardholder-specific and data that is common to many cardholders. Variable data can, for example, be printed on an information-bearing layer of the ID card using thermal printing ribbons and thermal printheads.

## 20 *Image Processing*

In one embodiment of the invention, the inventors have found that different image processing techniques are used to preprocess an original image that is to be printed as a covert image (using, for example, a covert media) depending on whether the tonality of image reproduction (e.g., printing process) is bitonal (e.g., two tones  
25 such as black and white or a first color and second color) or monochromatic (e.g., shaded image, grayscale, etc.). The inventors also note that other optional factors to consider include the viewing methods used with the image, such as reflectance, transmissive characteristics (e.g., as discussed above with the UV glowing) and tactility.)

30 For the methods discussed below, assume that an image is in digital form, such as resulting from being digitally captured, e.g., via a digital camera, optical sensor, etc., or through scanning a photograph with a scanner, etc. In at least some embodiments of

- 15 -

the invention, we provide methods to refine this captured image to produce an intermediate image, which can be transferred or printed (or used to generate an image to be transferred or printed) to the identification document as covert image 14.

Mass Transfer Images

5           In one embodiment, the invention provide a method that can be particularly well suited for producing bitonal images (e.g., black and white images), such as produced through mass-transfer thermal printing and Laser Xerography. Generally, in this embodiment, we process a captured image to bring-out or otherwise enhance relevant features found in the captured image. Relevant features of a human face may include  
10 the face outline, nose and mouth pattern, ear outline, eye shape, eye location hairline and shape, etc., or any other feature(s) that have been deemed to be relevant for identification purposes (e.g., particular features used with matching algorithms such as facial recognition algorithms). Once identified, these featured can be “thickened” or otherwise emphasized. The emphasized features can then form a digital version of a  
15 covert image, which can be transferred to an identification card.

The following discussion proceeds with reference to the accompanying flow diagrams and Figures and images (FIGS. 5a-5g) that variously correspond to our inventive processes.

FIG. 1 illustrates an identification document (ID) 8 in accordance with one  
20 embodiment of the invention, including an image 10 that is visible under normal viewing conditions. The ID document 8 can be formed using a core material such as PVC, TESLIN, polycarbonate (PC), Image 10 is preferably a color image, but the present invention is not limited to such. The document optionally includes ghost image 12, which can be a screened-back or “Ghost” version of image 10. Ghost image 12 is  
25 also preferably visible under normal viewing conditions. Covert image 14 (which is shown to be visible for illustrative purposes only) preferably corresponds to image 10 and is preferably an image that is not visible under “normal” viewing conditions.

We note that in an alternative embodiment, the identification document 8 need not include all three of the images 10, 12, and 14. For example, in one embodiment,  
30 the identification document 8 can only include covert image 14. In another embodiment, the identification document includes both covert image 14 and image 10.



- 16 -

(Note that FIG. 1 is illustrated as if covert image 14 is undergoing appropriate stimulation of the covert image (or, if the covert image is an optically variable image, is being held at an angle if printed with optical variable ink), since covert image 14 is illustrated as being visibly perceptible. It should be also appreciated that the present invention encompasses identification documents including more or less features than the illustrated document in FIG. 1. Additional features may include bar codes, magnetic stripes, digital watermarks, signatures and biometric information (e.g., fingerprint, etc.). These features, along with the positioning or embedding of the features, are optional, and are not required to practice the present invention.)

10           In one embodiment of the invention, covert image 14 is an ultraviolet (UV) image, meaning that it glows (e.g., visibly fluoresces or emits radiation) in response to appropriate UV stimulation. (In some implementation, the UV fluoresces in the UV spectrum upon excitation with visible light.). Covert image 14 is generally imperceptible under normal (e.g., non-ultraviolet or non-angle) viewing conditions

15           In one embodiment of the invention, covert image 14 is an infrared (IR) image, meaning that it glows (e.g., visibly fluoresces or emits radiation) in response to appropriate IR stimulation. In one embodiment of the invention, covert image 14 is a thermachromic image, meaning that it becomes visible only when the image (or entire ID document 8) is subject to a predetermined change in temperature, such as by heating or cooling. In one embodiment of the invention, covert image 14 is an optically variable image, meaning that covert image 14 is most visible when viewed at an angle. In one embodiment of the invention, covert image 14 is formed using a material such as a ferrofluid (available from FerroTec of Nashua, New Hampshire). Ferrofluids are responsive to magnetic fields, and we anticipate that ferrofluids can be used to produce covert images that become visible when an appropriate magnetic field is applied to the ferrofluid.

25           In one embodiment of the invention, covert image 14 is a combination of any one or more of UV, IR, thermachromic, ferrofluidic, and/or optically variable images. For example, covert image 14 can be both a UV and a thermachromic image by printing the card area, using the methods described herein, with both UV and thermachromic inks, meaning that when subject to appropriate stimulation, the normally “blank” area of the card will display either a UV image (if appropriate UV

30

- 17 -

stimulation is provided) or a thermachromic image (if appropriate temperature is provided). Those skilled in the art will appreciate that many combinations are possible. It is even envisioned that combination type inks, such as UV thermachromic inks (meaning inks that, to display an image, require *both* UV and appropriate temperature),  
5 the methods described herein will be usable with such inks.

FIG. 2 illustrates a first implementation of a method to emphasize particular image features, in accordance with one embodiment of the invention. As an initial step, we can improve the contrast in a captured image (step 20). For example, FIG. 5a illustrates such a captured image – a headshot corresponding to a human subject –  
10 while FIG. 5b corresponds to a contrast improved version of FIG. 5a, after the processing of step 20. For example, step 20 is intended to make dark pixels relatively darker and light pixels relatively lighter so as to increase the contrast of the image. Image processing methods to improve contrast are well known to those skilled in the art and not detailed here.

15 In addition, it should be noted that although FIGS. 5a and 5b are color images, the present invention is not limited to such. Indeed, our inventive techniques apply to black and white images as well. FIG. 5a preferably corresponds to image 10 (FIG. 1). Although not required, step 20 is capable of improving the performance of subsequent steps, such as the edge detection step 24. In some implementations of the invention, as  
20 a second step, the contrast-improved image (FIG. 5b) can be converted to a monochromatic image, e.g., a gray-scale image (step 22).

We analyze the contrast-enhanced image to identify or detect edges and/or boundaries within the image in step 24. As noted, eyes, nose and mouth often include prominent edges. Our preferred edge detection algorithm is the Sobel algorithm,  
25 however, we note that many other conventional algorithms such as other gradient-based edge detection algorithms (e.g., Roberts, Prewitt), Laplacian (e.g., Morriss-Hildreth) and the Canny edge algorithm can be suitably interchanged with this aspect of the present invention, as will be appreciated by those skilled in the art. Such algorithms are described, for example, in Alan Watt and Fabio Policarpo, The Computer Image,  
30 (Addison Wesley 1998) at p. 247-249, and also in many U.S. patent documents, such as U.S. patent nos. 6526161 and 4443438. The results of an edge detector produce an outline-like image, which highlights the edges (or maybe just the significant edges) of

- 18 -

the monochromatic image. If using a Sobel algorithm, or another algorithm that produces multiple planes, a horizontal edge plane (FIG. 5c) and a vertical edge plane (FIG. 5d) are produced. These horizontal and vertical planes (or sub-images) can be combined to produce a composite image as in step 26. Of course, step 26 can be  
5 skipped if the edge detection algorithm used in step 24 provides a composite horizontal and vertical edge image, instead of separate horizontal and vertical sub-images.

The composite image is then smeared, thickened or otherwise emphasized in step 28 (FIG. 5e). For example, in one embodiment, we can “grow” the edges by a predetermined factor (e.g., 1 ½ - 2 times the original edge or line thickness). In one  
10 embodiment, we can use an iterative pasting of each sub-image or image plane, multiple times onto a final composite image, but each time offsetting the sub-image by a few pixels (e.g., in a range of 2-5 pixels). In one embodiment, once a composite image is formed, the composite image can be repeatedly copied onto itself, but offset in different directions (toward image corners, or along an X-Y axis, etc.).

15 In one embodiment of the invention, this thickened image (FIG. 5e) serves as the master (or negative) for guiding printing of UV covert image 14. In one embodiment of the invention, the thickened image is binaryized or converted to a bitonal image (FIG. 5f) to guide the printing of covert image 14 (step 29). In one embodiment of the invention, the thickened image or bitonal image is first inverted  
20 (FIG. 5g), and the inverted image guides the printing of covert image 14. (So, FIG. 5G could be printed as the covert image 14.).

We have found that the method of FIG. 2 can be capable of significantly reducing the washing-out of image details experienced in conventional covert images such as UV, IR, or thermachromic images (when fluorescing or otherwise being  
25 stimulated).

An alternative implementation of the invention is discussed with reference to FIG. 3. We improve the contrast in a captured image (step 30). Here again, FIG. 5a illustrates such a captured image – a headshot corresponding to a human subject – while FIG. 5b corresponds to a contrast improved version of FIG. 5a. As previously  
30 noted, step 30 emphasizes the contrast of an image, e.g., by making dark pixels relatively darker and light pixels relatively lighter (step 30 of FIG. 3 is similar to step

- 19 -

20 of FIG. 2). Our contrast-enhancing step 30 is capable of improving the performance of subsequent steps in FIG. 3, such as the edge detection step 34.

Referring again to FIG. 3, in step 34, we analyze the contrast-enhanced image to identify or detect edges and/or boundaries within the image (step 34 of FIG. 3 is  
5 substantially similar to step 24 of FIG. 2). Virtually any edge detection algorithm is usable for step 34. As noted, facial features such as eyes, nose, hair details and mouth often include prominent edges. The results of an edge detector produce an outline-like image, which highlights the edges (or in some implementations just significant edges) of the contrast-enhanced image. If using a Sobel algorithm, or another algorithm that  
10 produces multiple planes, a horizontal edge plane (FIG. 5c) and a vertical edge plane (FIG. 5d) are produced. The results of the edge detection are provided to form a composite image (e.g., step 36; FIG. 5e).

The composite image of step 36 is used to guide printing (step 38). In some implementations we convert the composite image into a binaryized or bitonal image  
15 (e.g., FIG. 5f). We can also invert a binaryized or bitonal image (e.g., resulting in FIG. 5g) to guide printing. We have found that the method of FIG. 3 method is also capable of reducing the washing-out of image details experienced in conventional covert images (e.g., UV, IR, thermachromic) images when the images are appropriately stimulated to become visible (e.g., when fluorescing for UV images).

## 20 Monochromatic

With reference to FIG. 4, a method for enhancing UV images formed through, e.g., D2T2, is described. An originally captured image is processed to increase the contrast in the captured image or in selected areas of the original image (step 40). (In  
25 one embodiment, the invention uses an edge-detection algorithm to identify selected areas (e.g., eyes, nose, mouth, face shape, etc.) in the original image, and the contrast in only these selected areas is increased.). We note that care should be taken when using image-adaptive software to avoid removing pixel-intensity information that contributes to the quality of a final image. Dithering (e.g., the Floyd Stein dithering method or other conventional dithering methods (e.g., Floyd Stein, Burkes, Ordered dithering,  
30 Stucki, Stephens, Sierra and Jarvis, as are known to those skilled in the art )) of the contrast-adjusted image is employed (step 42) to produce a print-ready image usable as

- 20 -

a printing master (step 44). The dithering helps to minimize the effects of UV washout. The dithered image is used as a master for printing a corresponding UV image (step 44). In one embodiment, we invert the dithered image, and then guide printing with the dithered image. As an optional step (not shown in FIG. 4), we scale the contrast-  
5 adjusted image to a size that it will be printed, prior to step 42. Those skilled in the art will appreciate that many conventional algorithms and products are usable to scale the contrast-adjusted image to a desired size.

In one embodiment of the invention, we embed a steganographic code into the covert image 14. For example, steganographic code can be embedded into a covert UV  
10 image 14. The code can be embedded in the master image, e.g., image 5g. Or the code can be embedded in perceptually significant features, e.g., facial outlines, hair, etc. that are able to survive the processing of FIGS. 2 and 3.

One form of steganographic encoding is digital watermarking. Digital watermarking is a process for modifying physical or electronic media to embed a  
15 machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. In some embodiments, the identification document includes two or more digital watermarks.

Digital watermarking systems typically have two primary components: an  
20 encoder that embeds the digital watermark in a host media signal, and a decoder that detects and reads the embedded digital watermark from a signal suspected of containing a digital watermark (a suspect signal). The encoder embeds a digital watermark by altering the host media signal. The reading component analyzes a suspect signal to detect whether a digital watermark is present. In applications where the digital  
25 watermark encodes information, the reader extracts this information from the detected digital watermark. The reading component can be hosted on a wide variety of tethered or wireless reader devices, from conventional PC-connected cameras and computers to fully mobile readers with built-in displays. By imaging a watermarked surface of the card, the watermark's "payload" can be read and decoded by this reader.

30 Several particular digital watermarking techniques have been developed. The reader is presumed to be familiar with the literature in this field. Some techniques for embedding and detecting imperceptible watermarks in media signals are detailed in the

- 21 -

assignee's co-pending U.S. Patent Application No. 09/503,881, U.S. Patent No. 6,122,403 and PCT patent application PCT/US02/20832.

Returning to the present implementation, in accordance with this embodiment of the invention, a digital watermark is embedded in the covert image 14. For purposes of illustration, assume that the covert image 14 is a UV image printed in accordance with any of the methods of FIGs. 2 through 4 herein. A watermark detector can only read the covert UV watermark if the host identification document 8 is subject to appropriate UV stimulation at the same time that the host identification document is presented to the watermark detector. This provided additional security to the identification document 8, because even if a counterfeiter is able to access UV inks to print a bogus covert image 14, the bogus covert image 14 will not contain the embedded digital watermark. Of course, mere photocopying or scanning of the identification document 8 will similarly frustrate the counterfeiter, who will be unable to reproduce, through scanning or photocopying, either the covert image 14 or the watermark contained therein.

In one embodiment, the watermark embedded in the covert image 14 may include a payload or message. The message may correspond, e.g., to the ID document number, printed information, issuing authority, biometric information of the bearer, and/or database record, etc. The watermark embedded in the covert image 14 may also include an orientation component, to help resolve image distortion such as rotation, scaling and translation. In at least one embodiment of the invention, we embed two or more watermarks in the OVD image.

In further embodiments, the watermark embedded in the covert image 14 corresponds to information printed on the ID document, or to information carried by a second watermark embedded elsewhere on the ID document (e.g., background pattern, image 10, etc.). More techniques for digital watermarks and ID cards can be found in Digimarc's U.S. Provisional Patent application no. 60/421,254, U.S. Patent Application No. 10/094,593, and in U.S. Patent No. 5,841,886. We expressly contemplate that the techniques disclosed in this application can be combined with the aspects of the present invention.

Concluding Remarks

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms, and in many different environments.

5           The technology disclosed herein can be used in combination with other technologies. Also, instead of ID documents, the inventive techniques can be employed with product tags, product packaging, labels, business cards, bags, charts, smart cards, maps, labels, etc., etc. The term ID document is broadly defined herein to include these tags, maps, labels, packaging, cards, etc.

10           It should be appreciated that while FIG. 1 illustrates a particular species of ID document -- a driver's license -- the present invention is not so limited. Indeed our inventive methods and techniques apply generally to all identification documents defined above. Moreover, our techniques are applicable to non-ID documents, e.g., such as printing or forming covert images on physical objects, holograms, etc., etc.

15           Further, instead of ID documents, the inventive techniques can be employed with product tags, product packaging, business cards, bags, charts, maps, labels, etc., etc., particularly those items including providing a non-visible indicia, such as an image information on an over-laminate structure. The term ID document is broadly defined herein to include these tags, labels, packaging, cards, etc. In addition, while some of  
20           the examples above are disclosed with specific core components, it is noted that laminates can be sensitized for use with other core components. For example, it is contemplated that aspects of the invention may have applicability for articles and devices such as compact disks, consumer products, knobs, keyboards, electronic components, decorative or ornamental articles, promotional items, currency, bank  
25           notes, checks, etc., or any other suitable items or articles that may record information, images, and/or other data, which may be associated with a function and/or an object or other entity to be identified.

          It should be understood that while our some of our detailed embodiments described herein use UV inks and/or dyes by way of example, the present invention is  
30           not so limited. Our inventive techniques and methods will improve the visibility and crispness of infrared and other fluorescing images as well. The inventive techniques and methods can improve the visibility and crispness of thermachromic inks and resins

- 23 -

(i.e., inks and resins whose appearance changes and/or becomes visible with temperature changes). Moreover, our inventive techniques are useful for preprocessing images destined for ID documents using various printing processes including, but not limited to, dye infusion, mass-transfer, laser xerography, ink jet, wax transfer, variable dot transfer, and other printing methods by which a fluorescing image can be formed.

It should be appreciated that the methods described above with respect to FIGS. 1-5, as well as the methods for implementing and embedding digital watermarks, can be carried out on a general-purpose computer. These methods can, of course, be implemented using software, hardware, or a combination of hardware and software.

We note that some image-handling software, such as Adobe's PrintShop, as well as image-adaptive software such as LEADTOOLS (which provide a library of image-processing functions and which is available from LEAD Technologies, Inc., of Charlotte, North Carolina) can be used to facilitate these methods, including steps such as providing enhanced contrast, converting from a color image to a monochromatic image, thickening of an edge, dithering, registration, etc. An edge-detection algorithm may also be incorporated with, or used in concert with, such software. Computer executable software embodying the FIGS. 2-4 steps, or a subset of the steps, can be stored on a computer readable media, such as a diskette, removable media, DVD, CD, hard drive, electronic memory circuit, etc.).

To provide a comprehensive disclosure without unduly lengthening the specification, applicants hereby incorporate by reference each of the U.S. patent documents referenced above.

The technology and solutions disclosed herein have made use of elements and techniques known from the cited documents. Other elements and techniques from the cited documents can similarly be combined to yield further implementations within the scope of the present invention. Thus, for example, single-bit watermarking can be substituted for multi-bit watermarking, technology described as using imperceptible watermarks or encoding can alternatively be practiced using visible watermarks (glyphs, etc.) or other encoding, local scaling of watermark energy can be provided to enhance watermark signal-to-noise ratio without increasing human perceptibility, various filtering operations can be employed to serve the functions explained in the prior art, watermarks can include subliminal graticules to aid in image re-registration,



- 24 -

encoding may proceed at the granularity of a single pixel (or DCT coefficient), or may similarly treat adjoining groups of pixels (or DCT coefficients), the encoding can be optimized to withstand expected forms of content corruption, etc. Thus, the exemplary embodiments are only selected samples of the solutions available by combining the

5 teachings referenced above. The other solutions necessarily are not exhaustively described herein, but are fairly within the understanding of an artisan given the foregoing disclosure and familiarity with the cited art. The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the

10 interchanging and substitution of these teachings with other teachings in this and the referenced patent documents are also expressly contemplated.

- 25 -

What is claimed is:

1. A method of processing a digital image that is to be printed on a surface of an  
5 identification document as a covert image, comprising:  
detecting at least one of edges and boundaries within the image, the detected edges or boundaries forming an intermediate image; and  
emphasizing the edges or boundaries within the intermediate image.
- 10 2. The method of claim 1, wherein emphasizing further comprises iteratively copying the intermediate image onto itself, wherein each iterative copy is offset with respect to the original intermediate image.
- 15 3. The method of claim 2, wherein the offset comprises a range of 2-5 pixels.
4. The method of claim 1, wherein emphasizing comprises growing the edges or boundaries by a predetermined thickness.
- 20 5. The method of claim 1, wherein detecting edges comprises generating a horizontal edge image comprising horizontal edge components and generating a vertical edge image comprising vertical edge components.
- 25 6. The method of claim 5, further comprising summing the horizontal edge image and the vertical edge image, the sum comprising the intermediate image.
- 30 7. The method of claim 6, wherein emphasizing comprises iteratively pasting copies of the horizontal edge image and vertical edge image onto the intermediate image, wherein each iteratively pasted horizontal edge image and each vertical edge image is offset with respect to a first placed horizontal edge image and a first placed vertical edge image, respectively.

- 26 -

8. The method of claim 1, further comprising increasing the contrast in the image prior to detecting the at least one of edges and boundaries within the image.

9. The method of claim 1, further comprising printing the emphasized image in  
5 a covert medium on an identification document.

10. The method of claim 9, wherein the covert medium comprises at least one of an ultraviolet printing medium, an infrared printing medium, a thermachromic printing medium, a ferrofluidic printing medium, and an optically variable printing  
10 medium.

11. The method of claim 9, wherein prior to printing, the emphasized intermediate image is converted to a bitonal image.

15 12. The method of claim 11 further comprising inverting the image prior to printing.

13. The method of claim 12, further comprising printing the inverted bitonal image as a covert image on an identification document.

20

14. A method of providing a covert image to an identification document, comprising:

increasing contrast in at least a portion of a digital image;

dithering the contrast-increased portion of the digital image; and

25

transferring the dithered image to the identification document.

15. The method of claim 14 further comprising, prior to increasing contrast, detecting at least one of edges and boundaries within the digital image, the at least one of detected edges and boundaries comprising the portion of the digital image that has  
30 had its contrast increased.

- 27 -

16. The method of claim 14 wherein the covert image, once transferred to the identification document, is generally visibly perceptible only when exposed to a stimulus adapted to enable the covert image to be viewed by a human eye.

5           17. The method of claim 14 wherein transferring the dithered image to the identification document comprises printing the dithered image on the identification document using a covert medium, the covert medium comprising at least one of an ultraviolet printing medium, an infrared printing medium, a thermachromic printing medium, a ferrofluidic printing medium, and an optically variable printing medium.

10

18. A method to reduce at least one of image washout and blurring caused by the fluorescence of a covert image that is to be transferred to an identification document, said method comprising, prior to the transfer of the covert image:

15           receiving a digital image that is to be used as a model to generate the covert image;

          increasing contrast in the digital image;

          detecting edges or boundaries within the image, the detected edges or boundaries forming an intermediate image; and

          emphasizing the edges or boundaries within the intermediate image.

20

19. The method of claim 18, wherein emphasizing comprises iteratively copying the intermediate image onto itself, wherein each iterative copy is offset with respect to the original intermediate image.

25

20. The method of claim 19, wherein the offset a range of 2-5 pixels.

21. The method of claim 18, wherein emphasizing comprises growing at least one of the edges and boundaries by a predetermined thickness.

30

22. The method of claim 18, wherein detecting edges comprises generating a horizontal edge image comprising horizontal edge components and generating a vertical edge image comprising vertical edge components.

23. The method of claim 19, further comprising the step of summing the horizontal edge image and the vertical edge image, the sum comprising the intermediate image.

5

24. The method of claim 18, wherein emphasizing step comprises iteratively pasting copies of the horizontal edge image and vertical edge image onto the intermediate image, wherein each iteratively pasted horizontal edge image and each vertical edge image is offset with respect to a first placed horizontal edge image and a first placed vertical edge image, respectively.

10

25. The method of claim 18, further comprising converting the emphasized intermediate image to a bitonal image and inverting the bitonal image.

15

26. The method of claim 25, further comprising printing the inverted bitonal image on the identification document with at least one covert medium.

27. An identification document comprising:

a core layer comprising a core material capable of having printed thereon an image formed using a covert medium;

20

a covert image printed to the core layer, the covert image formed by:

providing a digital image that is to be used as a model to generate the covert image;

increasing the contrast in the digital image;

25

detecting edges or boundaries within the digital image, the detected edges or boundaries forming an intermediate image;

emphasizing the edges or boundaries within the intermediate image; and

printing the emphasized intermediate image in a covert medium on the core layer.

30

28. An identification document, comprising:

- 29 -

a core layer comprising a core material capable of having printed thereon an image formed using a covert medium;

a covert image printed to the core layer, the covert image formed by:

5 providing a digital image that is to be used as a model to generate the covert image;

increasing contrast in at least a portion of the digital image;

dithering the contrast-increased portion of the digital image; and

transferring the dithered image to the identification document.

10 29. The identification document of claim 28, wherein said covert image comprises steganographic encoding.

30. The identification document of claim 29, wherein the steganographic encoding comprises a digital watermark.

15

31. The identification document of claim 27, wherein said covert image comprises steganographic encoding.

20 32. The identification document of claim 31, wherein the steganographic encoding comprises a digital watermark.

33. The identification document of claim 29, wherein the core comprise at least one of Teslin, polycarbonate, PVC, and a plastic.

25 34. A method of producing an identification document comprising:  
receiving a digital image;  
processing the digital image to emphasize a set of image features; and  
printing the processed digital image on the identification document using at  
least one covert printing medium, the covert printing medium being visible to a human  
30 eye only upon application of a predetermined stimulus.

- 30 -

35. The method of claim 34, wherein the processing helps alleviate at least one of image blurring and washout of the digital image printed with the covert printing medium.
- 5           36. The method of claim 34, wherein the sets of image features comprise at least one of eyes, mouth edges, face outline, ears and hair outline.

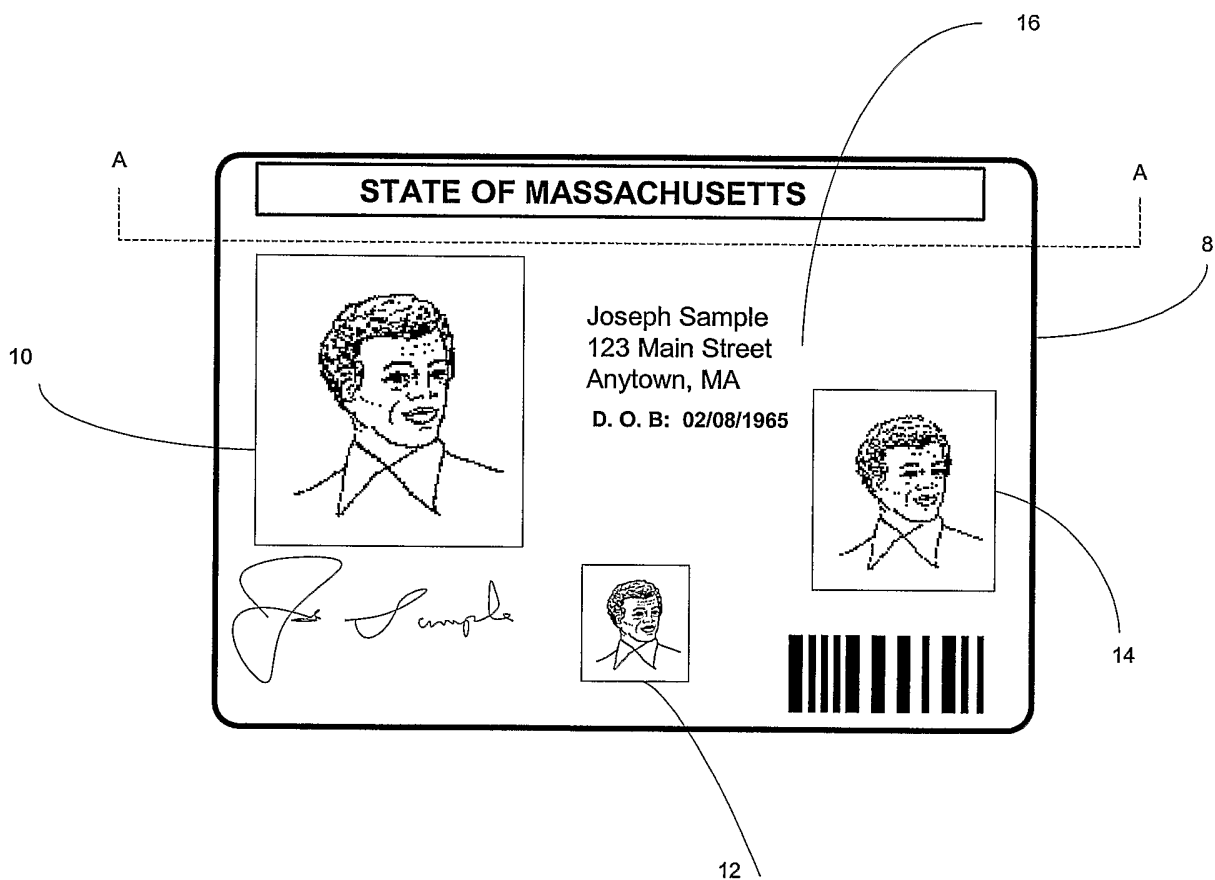


FIG. 1



FIG. 2

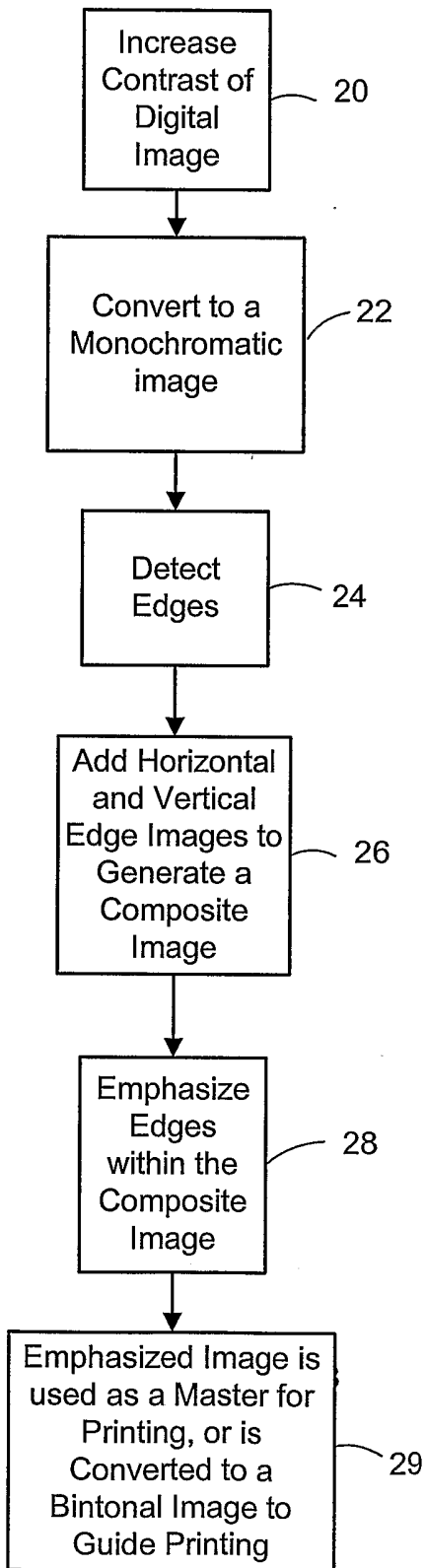
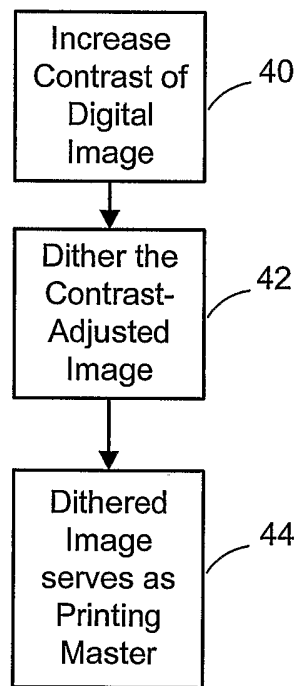


FIG. 4



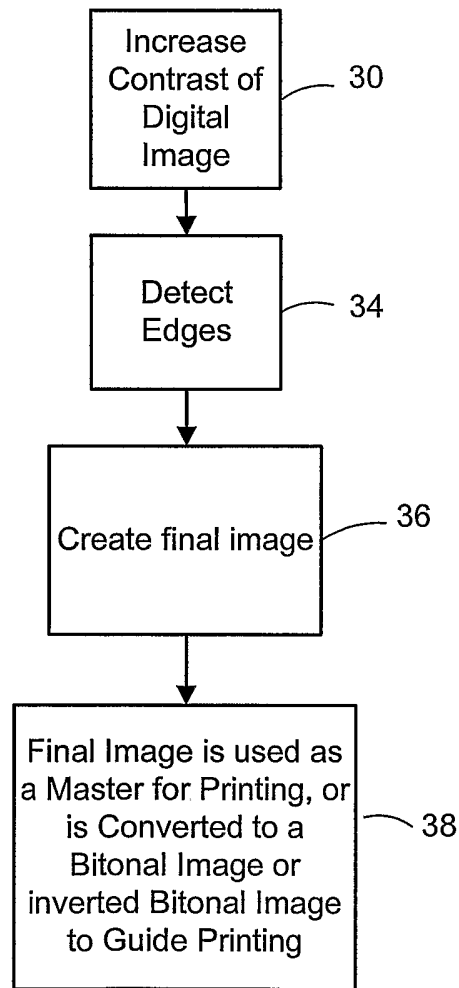


FIG. 3

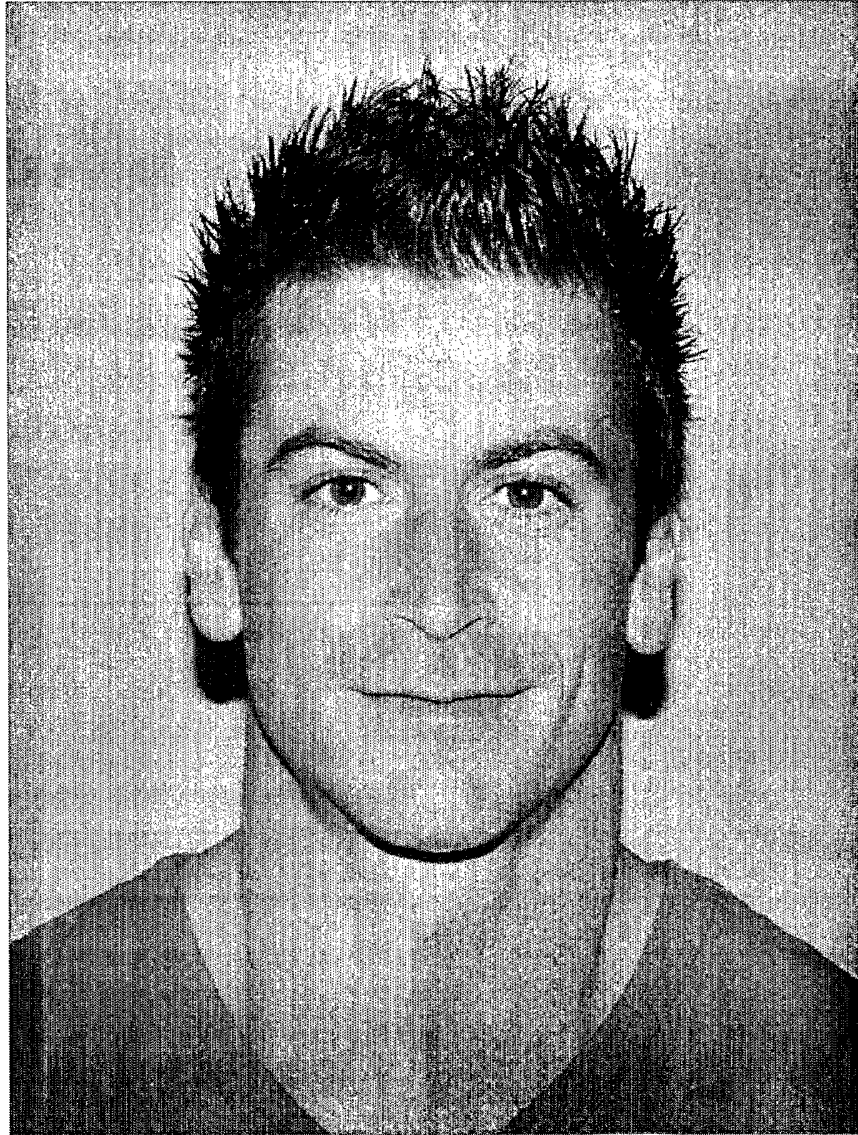


FIG. 5A

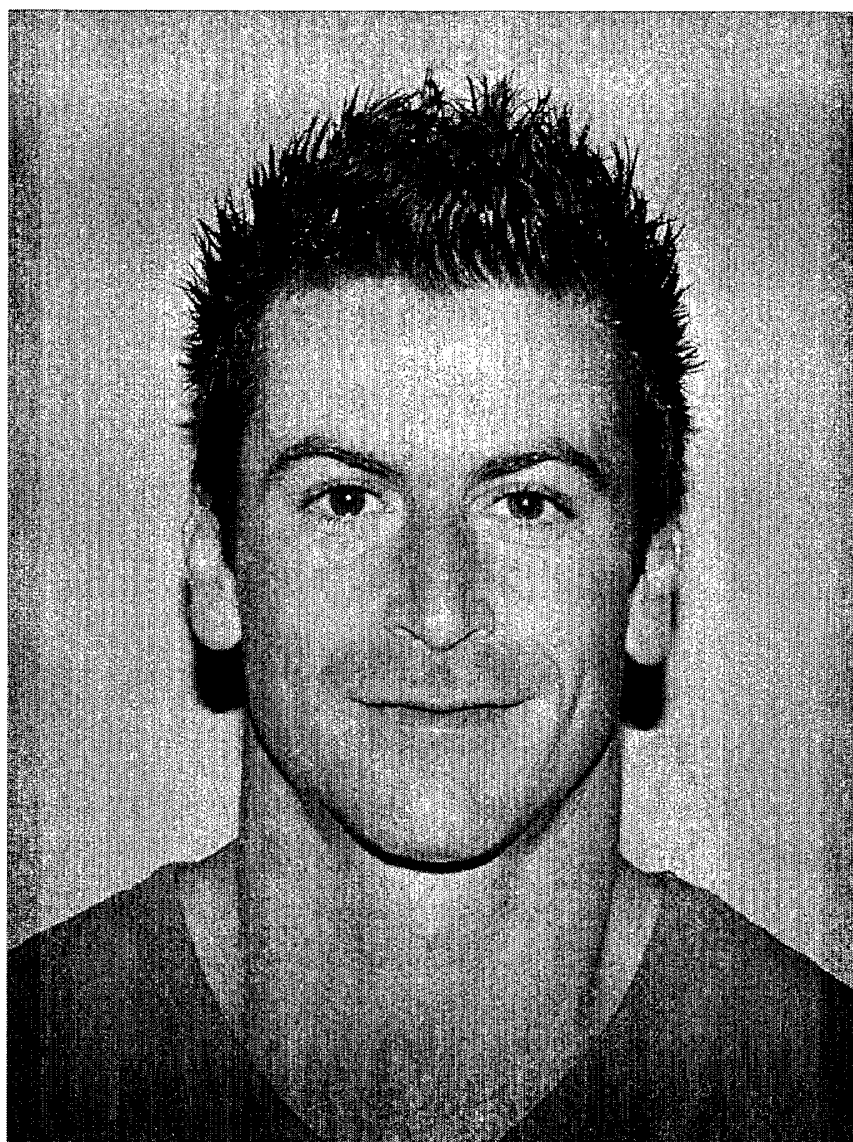


FIG. 5B



FIG. 5C

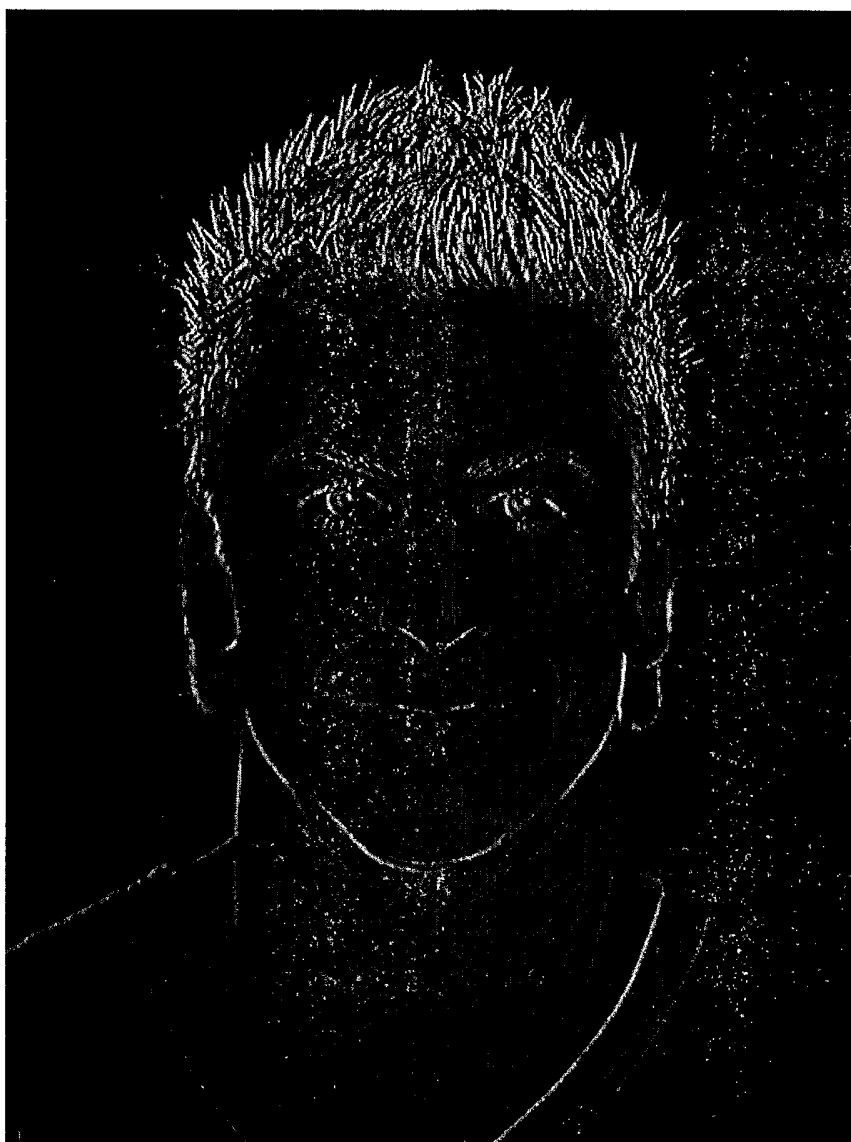


FIG. 5D

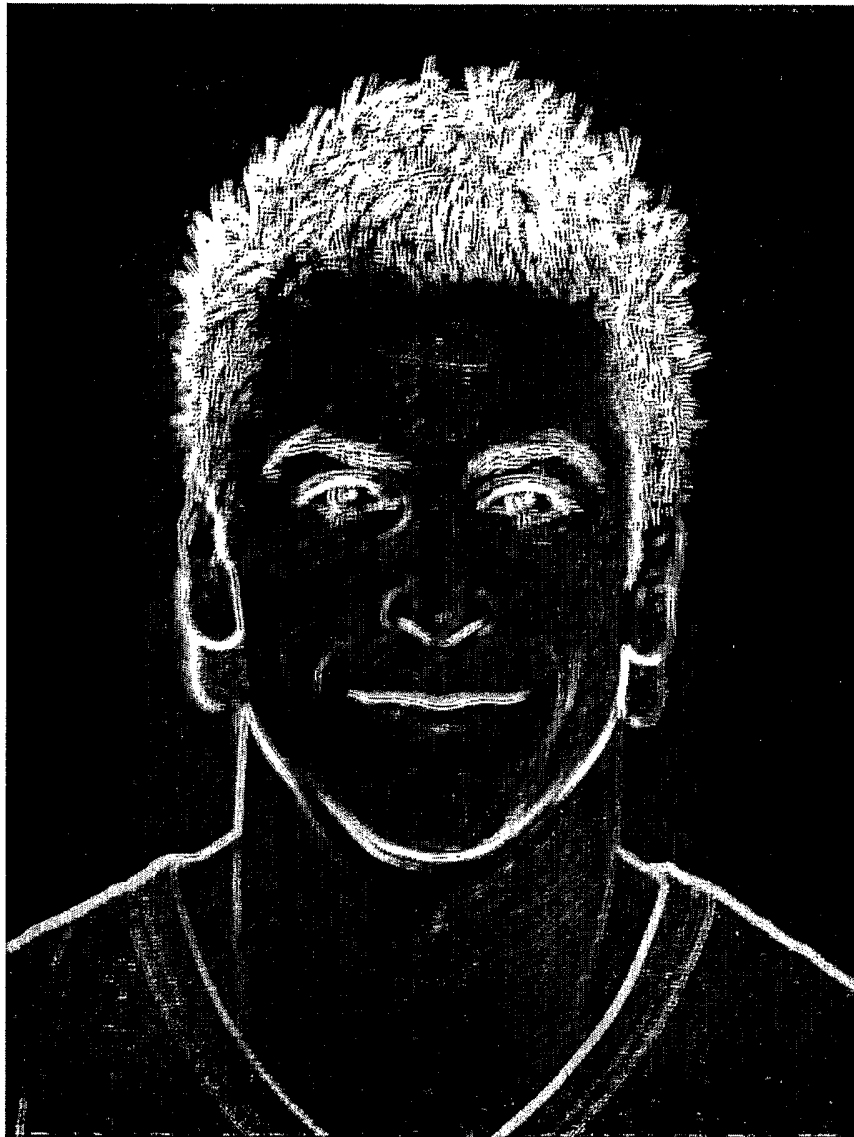


FIG. 5E



FIG. 5F



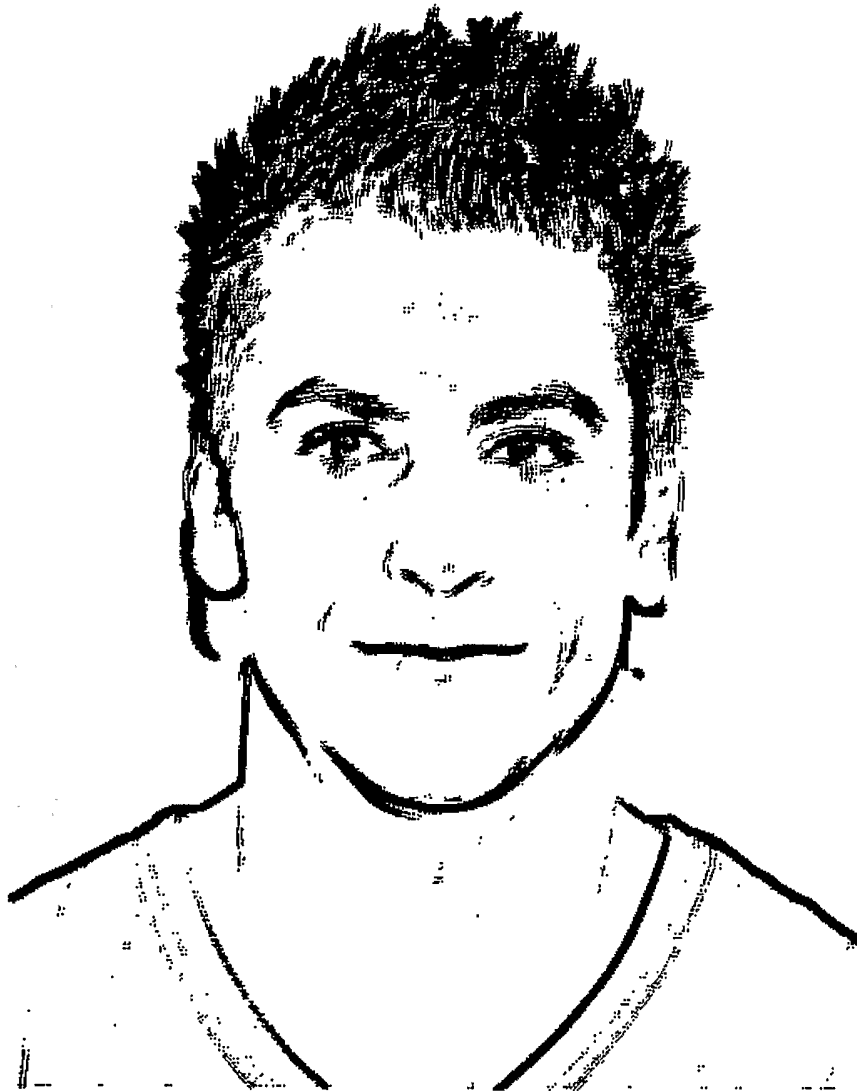


FIG. 5G