(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 918 300 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
08.01.2003 Bulletin 2003/02

(51) Int Cl.[7]: **G06K 9/00**

(21) Application number: **98120186.6**

(22) Date of filing: **29.10.1998**

(54) **Fingerprint feature correlator**

Merkmalkorrelator für Fingerabdrücke

Corrélateur de caractéristiques pour empreintes digitales

(84) Designated Contracting States:
DE FR GB IT

(30) Priority: **22.11.1997 US 995330**

(43) Date of publication of application:
26.05.1999 Bulletin 1999/21

(73) Proprietor: **TRW Inc.**
Redondo Beach, California 90278 (US)

(72) Inventors:
- **Hsu, Shi-Ping**
  Pasadena, CA 91107 (US)
- **Evans, Bruce W.**
  Redondo Beach, CA 90277 (US)

(74) Representative: **Schmidt, Steffen J., Dipl.-Ing.**
Wuesthoff & Wuesthoff,
Patent- und Rechtsanwälte,
Schweigerstrasse 2
81541 München (DE)

(56) References cited:
US-A- 4 646 352 **US-A- 5 067 162**

- **ANDERSON S: "A SINGLE CHIP SENSOR & IMAGE PROCESSOR FOR FINGERPRINT VERIFICATION" PROCEEDINGS OF THE CUSTOM INTEGRATED CIRCUITS CONFERENCE, SAN DIEGO, MAY 12 - 15, 1991, no. CONF. 13, 12 May 1991 (1991-05-12), pages 12.1.1-12.1.4, XP000295730 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS ISBN: 0-7803-0015-7**
- **HIRONORI YAHAGI ET AL: "MOVING-WINDOW ALGORITHM FOR FAST FINGERPRINT VERIFICATION" TECHNOLOGIES TODAY AND TOMORROW, NEW ORLEANS, APRIL 1 - 4, 1990, vol. 1, 1 April 1990 (1990-04-01), pages 343-347, XP000203123 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
- **RATHA N K ET AL: "A REAL-TIME MATCHING SYSTEM FOR LARGE FINGERPRINT DATABASES" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, vol. 18, no. 8, 1 August 1996 (1996-08-01), pages 799-812, XP000632861 ISSN: 0162-8828**

EP 0 918 300 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This invention relates generally to pattern recognition systems and, more particularly, to a system and method for comparing two fingerprint images and determining whether or not they are from the same person. Fingerprints are, of course, widely used in criminal investigation work, and fingerprints are routinely taken from applicants for jobs, security clearances, citizenship, and so forth. For these and many other applications of fingerprint image processing, it is most often required to compare one fingerprint with many others, in an effort to find a match. So called "minutia matching" approaches are commonly used in such search applications. In these approaches a small amount of characteristic data is extracted from a fingerprint image. This data may be quickly compared with corresponding data from another image to determine if the imaged prints match. Extraction of this data is a complex process, and is relatively time consuming even on a powerful computer. For search applications, this is acceptable because the extracted minutia data are reused many times, so that the minutia extraction overhead is amortized over a large number of comparisons.

[0002] By way of contrast, the present invention pertains to the use of fingerprint images for purposes of verification of a person's identity. In this application, the person "enrolls" in a system by supplying a reference fingerprint image. When the same person's fingerprint image is subsequently scanned for purposes of gaining access to a protected property, the newly scanned image is compared with the reference image for verification. In many practical applications of fingerprint verification, such as for access to vehicles, buildings or computers, the process must be completed in a matter of seconds, preferably using an inexpensive computer processor.

[0003] Many fingerprint matching systems developed or proposed for verification purposes have followed much the same principles used in larger identification systems, using pattern minutia extraction and matching. Because the minutia extraction process involves complex and heterogeneous mathematical operations, and must be performed each time a finger is presented for verification, a powerful general-purpose computer processor is required in order to perform a comparison within an acceptable time. As a result, such systems are large in size and high in cost. Their application has therefore been limited, usually to the protection of important sites or computer installations for which the high cost is warranted and space is available.

[0004] Fingerprint image correlation is an alternative to minutia based approaches. It is attractive because correlation operations have a simple, repetitive mathematical structure, which is suited to implementation by custom computing hardware utilizing high levels of parallelism to achieve rapid processing. Such hardware can be realized compactly and inexpensively as an application specific integrated circuit (ASIC). U.S. Patent No. 5,067,162 to Driscoll, Jr. et al. Discloses a method and apparatus for verifying identity using fingerprint image correlation, but their apparatus is controlled by a programmable general purpose computer processor. Use of a programmable computer to implement the correlation of the two fingerprint images poses a difficult design choice between accuracy of results and speed of processing. In general, a high level of accuracy degrades the speed of processing to a degree that makes such a configuration unsuitable for many applications.

[0005] It will be appreciated from the foregoing that there is still a significant need for a fingerprint correlation technique that will operate rapidly and reliably, but which may be implemented in a compact package at relatively low cost. As will become apparent from the following summary, the present invention meets this need.

SUMMARY OF THE INVENTION

[0006] The present invention resides in a fingerprint feature correlator using a processing method that can be implemented in significant part in integrated circuitry, to provide fast processing without compromising reliability. It will be understood that the term "fingerprint" includes thumb print, palm print, and other similar biometric indicators used for identification.

[0007] Briefly, and in general terms, the fingerprint correlator of the invention comprises a fingerprint sensor, for generating a digital image of a fingerprint; an enrollment processor for extracting, from a fingerprint image generated by the fingerprint sensor from the fingerprint of an identified person, multiple reference patches that together uniquely identify the image; reference image storage means, for storing reference patch images and locations provided by the enrollment processor; a correlation processor for searching the subject fingerprint image generated by the fingerprint sensor from the fingerprint of a person seeking identity verification for instances of two dimensional pixel patterns sufficiently similar to the patterns of the stored reference patches, and for generating a set of candidate match locations in the subject image corresponding to the location of each such instance for each reference patch; and a geometric constraint checking processor, for attempting to locate in the set of candidate match locations a subset of locations that is geometrically congruent with a corresponding subset of reference patch locations, to a desired degree of accuracy, and for determining whether there is a match between the subject image and the stored reference image. The feature correlator also includes an image preprocessor, for converting the digital image of the fingerprint to binary form, removing extraneous background and, optionally, rotating the image to a standard orientation.

[0008] More specifically, the enrollment processor includes means for binarizing the gray scale digital image and thinning the binary image to obtain skeletal images of ridges and valleys in the fingerprint; means for ana-

lyzing the skeletal images to locate bifurcation features in the ridges and valleys; means for selecting reference patches based on feature density, and storing the reference patch locations in the reference image storage means; and means for extracting reference patch images from the skeletal images of the ridges and valleys and storing the reference patch images in the reference image storage means with the corresponding reference patch locations.

[0009] An important aspect of the invention is the correlation processor, which compares the pixels in every reference patch selected by the enrollment processor with the pixels in every possible patch location in the subject fingerprint image, to determine the locations of patches in the subject image that match, or nearly match, any of the reference patches. The correlation processor includes an array of correlator units, each for comparing a selected pixel from a reference patch with a selected pixel in the subject image, wherein the entire array simultaneously compares the selected pixel from each of a plurality of reference patches with a plurality of pixels in a block of pixels from the subject image; an address generator, for generating a sequence of addresses for accessing successive pixels in the plurality of reference patches, and another sequence of addresses for accessing successive blocks of pixels in the subject image, wherein each reference patch is compared with every possible patch position in the subject image; and a result collection memory, for recording pixel match count data pertaining to every possible match candidate position in the subject image, along with candidate match locations in the subject image. Preferably, the address generator further includes means for generating rotated reference patch addresses in such a way that a rotated image of each reference patch is also compared with each possible patch of the subject image. In particular, the means for generating rotated reference patch addresses includes means for storing multiple sets of two-dimensional offset addresses, each set of offset addresses defining a different rotation angle. By this means, each reference patch is compared with each possible patch of the subject image at multiple orientation angles.

[0010] Each correlator unit in the correlation processor includes a counter for recording a count indicative of the degree of match between a reference patch and a patch of the subject image; and the correlation processor further includes means for saving the contents of the counters in the result collection memory on completion of a comparison of all pixels in the reference patches, and means for saving a subject image location with each count, and means for resetting the counters to begin a comparison with other locations in the subject image. The correlation processor further includes means rendered operative at the conclusion of all matching operations of the correlation processor, for selecting a set of match candidates from the results saved in the result collection memory. The latter means for selecting a set of match candidates includes means for discarding match candidates that are positioned in the subject image relatively close to a better candidate.

[0011] Another important feature of the invention is the geometric constraint checking processor, which includes means for determining the distances between all possible pairs of reference patches; means for determining the distances between all possible pairs of distinct match candidates; means for selecting a feasible subset of the distinct match candidates such that the distances between all possible pairs in the feasible subset are approximately equal to the distances between corresponding pairs of reference patches; and means for declaring a match based on the size of the feasible subset.

[0012] The invention may also be defined in terms of a method for verifying a person's identity using fingerprint feature correlation. Briefly, the method comprises the steps of sensing a fingerprint of an identified person wanting to enroll a fingerprint image; generating a digital image of the fingerprint; enrolling the fingerprint image, by finding and extracting multiple reference patches that together uniquely identify the image; storing the extracted reference patch images and their locations in a reference image memory; sensing a subject fingerprint image of a person wanting identity verification; generating a digital subject fingerprint image from the sensed subject fingerprint image; searching the subject fingerprint image for instances of pixel patterns similar to the stored reference patch images, or with similar to rotated forms of the stored reference patches; generating a set of match candidates and their locations in the subject image; attempting to locate in the set of match candidates a subset of match candidates that is geometrically congruent with a corresponding subset of reference patches, to a desired degree of accuracy; and determining whether there is a match between the subject image and the stored reference image. The method as disclosed also includes preprocessing the digital image, by converting the digital image of the fingerprint to binary form, removing extraneous background picture elements, and optionally adjusting the image to a standard orientation.

[0013] More specifically, the enrolling step includes thinning the binary image to obtain skeletal images of ridges and valleys in the fingerprint; analyzing the skeletal images to locate bifurcation features in the ridges and valleys; selecting reference patches based on feature density; and extracting reference patch images from the skeletal images of the ridges and valleys.

[0014] The comparing step of the basic method includes comparing, in a correlator unit that is one member of an array of correlator units, a selected pixel from a reference patch with a selected pixel in the subject image, wherein the entire array simultaneously compares the selected pixel from each of a plurality of reference patches with a plurality of pixels in a block of pixels from the subject image; generating a sequence of addresses for accessing successive pixels in the plu-

rality of reference patches, and another sequence of addresses for accessing successive blocks of pixels in the subject image, wherein each reference patch is compared with every possible patch position in the subject image; and recording, in a result collection memory, pixel match count data pertaining to every possible match candidate position in the subject image, along with match candidate locations in the subject image. More specifically, the step of generating addresses further includes generating rotated reference patch addresses in such a way that a rotated image of each reference patch is also compared with each possible patch of the subject image. The step of generating rotated reference patch addresses includes storing multiple sets of two-dimensional offset addresses, each set of offset addresses defining a different rotation angle, and wherein each reference patch is compared with each possible patch of the subject image at multiple orientation angles.

[0015] Each step of comparing in a correlator unit includes recording a count indicative of the degree of match between a reference patch and a patch of the subject image; and the method further comprises the steps of saving the counts in the result collection memory on completion of a comparison of all pixels in the reference patches, saving a subject image location with each count, and resetting the counts to begin a comparison with other locations in the subject image. The method may also comprise the step, performed at the conclusion of all matching operations, of selecting a set of match candidates from the results saved in the result collection memory. This step of selecting a set of match candidates includes discarding match candidates that are positioned in the subject image relatively close to a better candidate.

[0016] Finally, the step of attempting to locate in the set of match candidates a subset of match candidates that is approximately geometrically congruent with a corresponding subset of reference patches, includes determining the distances between all possible pairs of reference patches; determining the distances between all possible pairs of distinct match candidates; selecting a feasible subset of the distinct match candidates such that the distances between all possible pairs in the feasible subset are approximately equal to the distances between corresponding pairs of reference patches; and declaring a match based on the size of the feasible subset. These distance tests do not preclude the possibility that the feasible subset is a mirror image of the corresponding reference locations, and, therefore, lacks the desired geometric congruency with the reference locations. Elimination of this possibility requires the incorporation of an additional test into the feasible set selection process.

[0017] It will be appreciated from the foregoing summary that the present invention represents a significant advance in the field of fingerprint image comparison for purposes of identity verification. In particular, the invention provides a reliable but very fast technique for comparing the distinguishing features of two fingerprint images Other aspects and advantages of the invention will become apparent from the following more detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018]

FIG. 1 is a block diagram showing the principal components of a fingerprint feature correlator in accordance with the present invention;

FIG. 2 is a flowchart showing the principal functions performed by the apparatus of the invention;

FIG. 3 is a binary image of a fingerprint with overlaid square outlines indicating reference patches chosen in an enrollment process to identify the fingerprint;

FIG. 4 is a set of trinary images of twenty-five reference patches that have been reduced to skeletal form, with white pixels indicating ridges and black pixels indicating valleys of the fingerprint pattern;

FIG. 5 is binary image of a different fingerprint of the same finger that was used to generate the image of FIG. 3, and also showing how the reference patches of FIG. 4 may be overlaid on the binary image to verify that the fingerprints are of the same finger;

FIG. 6 is a binary image of a totally different fingerprint, taken from a different person, and showing how only two of the reference patches of FIG. 4 may be successfully matched on the fingerprint image;

FIG. 7 is a more detailed flowchart of the image quality check and image processing steps of FIG. 2;

FIGS. 8 and 9 taken together are a more detailed flowchart of the enrollment functions depicted in FIG. 2;

FIG. 10 is a hardware block diagram of the feature correlator processor shown in FIG. 1;

FIG. 11 is a flowchart of the functions performed by the feature correlator processor of FIG. 10;

FIG. 12 is a diagram showing a reference patch in regular and rotated orientation, in relation to a reference data frame;

FIG. 13 is a diagram showing a subject image data frame and a reference patch that is translated and rotated with respect to the subject image data frame, in the course of the correlation process;

FIG. 14 is block diagram illustrating how the reference patch images are correlated with the subject image in the feature correlator processor of FIG. 1;

FIG. 15 is a schematic diagram of a correlator unit or sub-module within the feature correlator processor of FIG. 1;

FIG. 16 is a flowchart showing how match candidates as determined in the feature correlator are further processed to obtain a list of patch candi-

dates in the subject fingerprint image;
FIG. 17 is a flowchart of the functions performed in geometric constraint analysis applied to the list of patch candidates to make a final determination as to whether a subject fingerprint image matches a reference image generated during enrollment;
FIG. 18 is a more detailed flowchart of the geometric constraint analysis step of choosing a maximal feasible subset of distinct match candidates;
FIG. 19 is an illustrative match candidate matrix;
FIGS. 20A-20F are diagrams of all of the feasible canonical representations corresponding to the match candidate matrix of FIG. 19;
FIG. 21 is a flowchart of a search process for finding the size of a maximal feasible subset of candidate match locations in a subject fingerprint image; and
FIG. 22 is a flowchart showing more detail of the recursive procedure used in the search process of FIG. 21.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0019] As shown in the drawings by way of illustration, the present invention pertains to a method and apparatus for correlation of features in fingerprint images. Fingerprint image correlators in the past either relied on the extraction and matching of pattern minutia or, even when minutia matching was not used, required programmable computers that are too bulky, costly and much too slow for many practical applications, such as controlling access to vehicles.

[0020] In accordance with the present invention, a fingerprint image is correlated with a previously stored reference image in such a way that a reliable result is obtained very quickly, but using relatively inexpensive and compact components that can be installed in a variety of locations or in a portable device.

Overview of the invention:

[0021] In its simplest form, this invention utilizes a commercial fingerprint imaging device and a processing system that interfaces with this device to capture, store and process fingerprint images in digital form, and to perform a fingerprint verification function. This invention performs two principal operations: 1) enrollment, which includes extracting and storing reference data from a fingerprint image of a person whose identity is independently verifiable at the time of enrollment, and 2) verification, by comparing features of a new fingerprint image with the reference data stored during enrollment. To use the system, a person first enrolls. In this process, a fingerprint image is captured and reference data "patches" are extracted from this image and stored. The identity of an enrolled person can then be verified by comparing subsequently captured images to the stored reference data. The system may store reference data for more than one individual. In this case, provision is made to retrieve the appropriate data for verification, based on other identifying information supplied by the person, such as an account number or user name. In addition, the reference data may be stored integrally to the system that performs the verification, or may be stored on external media or devices. This includes "smart cards" or similar devices, which users would retain and would connect to the system when they wished to establish their identity.

[0022] The principal components of the fingerprint feature correlator are shown in FIG. 1. These include a fingerprint sensor, indicated by reference numeral 10, which may be of the capacitive or the optical type, an image pre-processor 12, a reference patch determination processor 14, reference image storage 16, a correlator processor 18, and a geometric constraint checking processor 20. In outline, the fingerprint image, which is initially a gray-scale image, is converted to a binary valued image in the image preprocessor 12, which also performs other pre-processing functions, to be described with reference to FIG. 7. In the enrollment process, the reference patch determination processor 14 then analyzes the binary fingerprint image to identify the positions of characteristic features. Smaller sub-images (or "patches") containing these features, or a subset of these sub-images, are then extracted from the complete fingerprint image. Image processing operations are applied to these sub-images, known as reference "patches," to enhance the reliability of the subsequently performed verification process. The reference patches are stored in the reference image storage 16 for use in the verification process.

[0023] In the verification mode of operation, the binary image from the image preprocessor 12 is transmitted to the correlator processor 18, which also retrieves the reference patch images from the reference image storage 16. Details of operation of the correlator processor 18 will be discussed below, but briefly the processor compares each reference patch to a binarized subject fingerprint image over a full range of positions and orientations, and attempts to find a set of one or more candidate match positions for each reference patch. The correlator processor 18, therefore, identifies for each reference patch those positions and orientations (if any) at which the reference patch is highly correlated with the subject image. These data are forwarded to the geometric constraint checking processor 20, which also retrieves reference patch positions from the reference image storage 16. The geometric constraint checking processor 20 analyzes these positions to find the maximum number of candidate match positions having relative positions that are similar to the relative positions of the reference patches. The decision to accept the verification print as a match to the reference data is based on this number.

[0024] As will be further discussed below, the correlator processor 18 in the preferred embodiment of the invention is implemented as an application specific in-

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.