ABSTRACT

A SYSTEM AND METHOD FOR HUMAN FACE IDENTIFICATION

The present invention in a preferred embodiment provides systems and methods involving a camera that captures input image, a DSP processor that detects a face from the input image, normalizes it and recognizes the face by calculating correlation coefficient and scale invariant feature transform, and a display device which displays information about the matched face.

We claim,

1. A method for identifying an individual from an input image comprising the steps of:

a) preprocessing the input image by histogram equalization and Gaussian filtering;

b) generating a facial image by detecting a face from said input image;

c) rotating said generated facial image in such a way that eyes are in a horizontal line;

d) comparing said generated facial image with a database of saved facial images using normalized correlation technique;

e) generating a sorted list which comprises of facial images from said database having normalized coefficient of correlation greater than a threshold;

f) building a Gaussian scale space and difference of Gaussian images for all scales of said generated facial image and said facial images from said sorted list;

g) detecting keypoints with a local extrema in the difference of Gaussian images for all scales, assigning orientations to the keypoints and computing feature descriptors for the keypoints;

h) comparing the feature descriptors of said face with the feature descriptors of said facial images by calculating Eucledian distance;

i) selecting a facial image with minimum Euclidean distance as matched face.

2. A system for recognition of a face comprising:

1) at least one DSP processor that runs the method from 1.

2) at least one camera that captures the said input image

3) at least one display device which displays information about the said matched face.

Dated this 9th day of April 2013

Signature :-
Name : TALELE, Kiran

Signature :-
Name : BAIRATHI, Neha

Signature :-
Name : DAGA, Rahul

Signature :-
Name : DARJI, Jignesh

Signature :-
Name : PANDA, Rekha

A SYSTEM AND METHOD FOR HUMAN FACE IDENTIFICATION

FIELD OF THE INVENTION:

This invention relates to the field of face recognition.

BACKGROUND OF THE INVENTION:

Face recognition is a biometric approach focusing on the same identifier that humans use primarily to distinguish one person from another: their faces. Properly designed systems installed in airports, multiplexes, and other public places can detect presence of criminals among the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning. Thus face recognition has attracted much attention in the past years.

Recognizing faces in computer vision is a challenging problem. The illumination problem, the pose problem, scale variability, images taken years apart, glasses, moustaches, beards, low quality image acquisition, partially occluded faces are some examples of the issues to deal with. Thus face recognition algorithms must exhibit robustness to variations in the above parameters. The existing techniques do not perform well in cases of different illumination, background or rotation.

Thus there is a need to address the above mentioned disadvantages. The present invention aims to address the above mentioned problems.

OBJECTS OF THE INVENTION:

The object of the invention is to provide a system and method for human face identification irrespective of variation in illumination as well as scale. It also aims to solve the problem of recognizing tilted faces. The invention aims to increase the efficiency of existing recognition system by eliminating false detections and rejections.

SUMMARY OF THE INVENTION:

The present invention in a preferred embodiment provides systems and methods involving a DSP processor that runs the face detection normalization and recognition algorithm, a camera that captures input image and a display device which displays information about the matched face.

The present invention in a preferred embodiment provides systems and methods to preprocess the input image, create a generated facial image by detecting a face from said input image, rotate said generated facial image in such a way that eyes are in a horizontal line, compare said generated facial image with a database of saved facial images using normalized correlation technique, generate a sorted list which comprises of facial images from said database having normalized coefficient of correlation greater than a threshold, build a Gaussian scale space and difference of Gaussian images for all scales of said generated facial image and said facial images from said sorted list, detect keypoints with a local extrema in the difference of Gaussian images for all scales, assign orientations to the keypoints and computing feature descriptors for the keypoints, compare the feature descriptors of said face with the feature descriptors of said facial images by calculating Eucledian distance, select a facial image with minimum Euclidean distance as matched face.

BRIEF DESCRIPTION OF THE DRAWINGS:

Figure 1 provides an example of the working of the invention in a flowchart.

Figure 2 provides the steps of scale invariant feature extraction in a flowchart.

DESCRIPTION OF THE INVENTION:

In accordance with the embodiment of this invention, Figure 1 illustrates exemplary steps to identify human faces.

First the image is preprocessed(1) using histogram equalization based on grey level grouping to enhance low contrast images and Gaussian filtering to filter the noise. Face detection(2) is performed on the filtered image using Haar cascade classifier that is trained for human faces. The haar-like features of the filtered image is compared with the trained classifier and the face is detected.Face Normalization(3) includes eye detection(4) using Haar cascade classifier that is

trained for eyes. In geometric normalization(5), the slope of the line joining the two eyeballs is calculated and used to rotate the face in either anti-clockwise or clockwise direction based on the angle of rotation. The co-efficient of correlation(6) of the normalized image with each database image is calculated and the images having correlation co-efficient greater than the threshold is listed in another database. Then, the Scale Invariant Feature Transform(7) is performed on the input image.

Figure 2 illustrates the steps involved in Scale Invariant Feature Extraction of the input image and matching.

Creation of scale-space(8) is done by generating progressively blurred out images from the sample image, then reducing its size and blurring it again progressively until the desired number of octaves is achieved. In order to avoid introduction of new false details in the image, Gaussian blur function is used for blurring.

Mathematically, blurring is referred to as convolution of Gaussian operator and the image.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2}$$

Where

L : Blurred image, I : input image and G:Gaussian blur operator

x, y : location coordinates

σ: scale parameter/the amount of blur in an image

The amount of blurring in each successive image depends on scaling constant k. If the amount of blur in an image is σ, the amount of blur in next image will be $k*\sigma$.

The scale-variant features are eliminated by constructing a Difference of Gaussian pyramid(9). Two consecutive images in an octave are picked and one is subtracted from other. Then the next consecutive pair is taken and the process is repeated for all octaves. The resulting images are an approximation of scale invariant Laplace of Gaussian which efficiently detects stable keypoint locations in scale space.

The difference-of-Gaussian function D(x, y, σ) can be computed from the difference of Gaussians of two scales that are separated by a factor k:

$$D(x,y,\sigma) = \big(G(x,y,k\sigma) - G(x,y,\sigma)\big) * I(x,y) \simeq L(x,y,k\sigma) - L(x,y,\sigma)$$

This stage is to find the extrema points in the DOG pyramid. To detect the local maxima and minima of D(x, y, σ), each point is compared with its eight neighbors in the current image as well as the nine neighbors in the scale above and below it in the Difference of Gaussian pyramid i.e. each pixel is compared with a total of 26 other pixels. If the pixel represents a local maximum or minimum, it is selected as a candidate keypoint.

Removal of keypoints(11) is based on measures of their stability. During this stage low contrast points (sensitive to noise) and poorly localized points along edges (unstable) are discarded. Two criteria are used for the detection of unreliable keypoints.

The first criterion evaluates the contrast at each candidate keypoint. The function value at the extremum, D(x), is useful for rejecting unstable extrema with low contrast.

$$D(x)=D+\frac{1}{2}\frac{\partial D^T}{\partial x}\ x$$

If the value is below some threshold, which means that the structure has low contrast, the keypoint is removed. The second criterion evaluates the ratio of principal curvatures of each candidate key point to search for poorly defined peaks in the Difference-of-Gaussian function. For keypoints with high edge responses, the principal curvature across the edge will be much larger than the principal curvature along it. Hence, to remove unstable edge keypoints based on the second criterion, the ratio of principal curvatures of each candidate keypoint is checked. If the ratio is below some threshold, the keypoint is kept, otherwise it is removed.

By assigning a consistent orientation(12) to each keypoint based on local image properties, the keypoint descriptor can be represented relative to this orientation and therefore achieve invariance to image rotation. This approach contrasts with the orientation invariant descriptors in which each image property is based on a rotationally invariant measure. The scale of the keypoint is used to select the Gaussian smoothed image, L, with the closest scale, so that all computations are performed in a scale-invariant manner. For each image sample, L(x, y), at this

scale, the gradient magnitude, m(x, y), and orientation, θ(x, y), is precomputed using pixel differences:

$$m(x,y) = \sqrt{(\mathrm{L}(x+1,y) - \mathrm{L}(x-1,y))^2 + (\mathrm{L}(x,y+1) - \mathrm{L}(x,y-1))^2}$$

$$\theta(x,y) = \tan^{-1}\frac{(\mathrm{L}(x,y+1) - \mathrm{L}(x,y-1)}{(\mathrm{L}(x+1,y) - \mathrm{L}(x-1,y)}$$

An orientation histogram is formed from the gradient orientations of sample points within a region around the keypoint. It has 36 bins covering the 360 degree range of orientations. Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian-weighted circular window with a σ that is 1.5 times that of the scale of the keypoint. Peaks in the orientation histogram correspond to dominant directions of local gradients. The highest peak in the histogram is detected, and then any other local peak that is within 80% of the highest peak is used to also create a keypoint with that orientation. Therefore, for locations with multiple peaks of similar magnitude, there will be multiple keypoints created at the same location and scale but different orientations. Finally, a parabola is fit to the 3 histogram values closest to each peak to interpolate the peak position for better accuracy.

The keypoint descriptor(13) is created by first computing the gradient magnitude and orientation at each image point of the 16*16 keypoint neighborhood. This neighborhood is weighted by a Gaussian window and then accumulated into orientation histograms summarizing the contents over subregions of the neighborhood of size 4 * 4 with the length of each arrow corresponding to the sum of the gradient magnitudes near that direction within the region. Each histogram contains 8 bins, therefore each keypoint descriptor features 4 * 4 * 8 = 128 elements. The coordinates of the descriptor and the gradient orientations are rotated relative to the keypoint orientation to achieve orientation invariance and the descriptor is normalized to enhance invariance to changes in illumination.

When using the SIFT algorithm for object recognition, each keypoint descriptor extracted from the query (or test) image is matched(14) independently to the database of descriptors extracted from all training images. The best match for each descriptor is found by identifying its nearest neighbor (closest descriptor) in the database of keypoint descriptors from the training images.

The object in the database with the largest number of matching points is considered the matched object.

In an embodiment of the invention, a user may provide user input through any suitable input device or input mechanism such as but not limited to a keyboard, a mouse, a joystick, a touchpad, a virtual keyboard, a virtual data entry user interface, a virtual dial pad, a software or a program, a scanner, a remote device, a microphone, a webcam, a camera, a fingerprint scanner, pointing stick, or any combination thereof.

In an embodiment of the invention, the systems and methods can be practised using any electronic device which may be connected to one or more of other electronic device with wires or wirelessly which may use technologies such as but not limited to, Bluetooth, WiFi, Wimax. This will also extend to use of the aforesaid technologies to provide an authentication key or access key or electronic device based unique key or any combination thereof.

In an embodiment of the invention, the systems and methods can be practised using any electronic device which may contain or may be infected by one or more of an undesirable software such as but not limited to a virus, or a Trojan, or a worm, malware, spyware, adware, scareware, crimeware, rootkit or any combination thereof.

In an embodiment of the invention the system may involve software updates or software extensions or additional software applications.

In an embodiment of the invention one or more user can be blocked or denied access to one or more of the aspects of the invention.

The described embodiments may be implemented as a system, method, apparatus or article of manufacture using standard programming and/or engineering techniques related to software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a "computer readable medium", where a processor may read and execute the code from the computer readable medium. A computer readable medium may comprise

media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.). Still further, the code implementing the described operations may be implemented in "transmission signals", where transmission signals may propagate through space or through a transmission media, such as an optical fibre, copper wire, etc. The transmission signals in which the code or logic is encoded may further comprise a wireless signal, satellite transmission, radio waves, infrared signals, Bluetooth, etc. The transmission signals in which the code or logic is encoded is capable of being transmitted by a transmitting station and received by a receiving station, where the code or logic encoded in the transmission signal may be decoded and stored in hardware or a computer readable medium at the receiving and transmitting stations or devices. An "article of manufacture" comprises computer readable medium, hardware logic, and/or transmission signals in which code may be implemented. A device in which the code implementing the described embodiments of operations is encoded may comprise a computer readable medium or hardware logic. Of course, those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention, and that the article of manufacture may comprise suitable information bearing medium known in the art.

In an embodiment of the invention the term network means a system allowing interaction between two or more electronic devices, and includes any form of inter/intra enterprise environment such as the world wide web, Local Area Network (LAN) , Wide Area Network (WAN) , Storage Area Network (SAN) or any form of Intranet.

In an embodiment of the invention, the systems and methods can be practised using any electronic device. An electronic device for the purpose of this invention is selected from any device capable of processing or representing data to a user and providing access to a network or any system similar to the internet, wherein the electronic device may be selected from but not

limited to, personal computers, mobile phones, laptops, palmtops, portable media players and personal digital assistants.

In an embodiment of the invention, computer program code for carrying out operations or functions or logic or algorithms for aspects of the present invention may be written in any combination of one or more programming languages which are either already in use or may be developed in future, such as but not limited to Java, Smalltalk, C++, C, Foxpro, Basic, HTML, PHP, SQL, Javascript, COBOL, Extensible Markup Language (XML), Pascal, Python, Ruby, Visual Basic .NET, Visual C++, Visual C# .Net, Python, Delphi, VBA, Visual C++ .Net, Visual FoxPro, YAFL, XOTcl, XML, Wirth, Water, Visual DialogScript, VHDL, Verilog, UML, Turing, TRAC, TOM, Tempo, Tcl-Tk, T3X, Squeak, Specification, Snobol, Smalltalk, S-Lang, Sisal, Simula, SGML, SETL, Self, Scripting, Scheme, Sather, SAS, Ruby, RPG, Rigal, Rexx, Regular Expressions, Reflective, REBOL, Prototype-based, Proteus, Prolog, Prograph, Procedural, PowerBuilder, Postscript, POP-11, PL-SQL, Pliant, PL, Pike, Perl, Parallel, Oz, Open Source, Occam, Obliq, Object-Oriented, Objective-C, Objective Caml, Obfuscated, Oberon, Mumps, Multiparadigm, Modula-3, Modula-2, ML, Miva, Miranda, Mercury, MATLAB, Markup, m4, Lua, Logo, Logic-based, Lisp (351), Limbo, Leda, Language-OS Hybrids, Lagoona, LabVIEW, Interpreted, Interface, Intercal, Imperative, IDL, Icl, ICI, HyperCard, HTMLScript, Haskell, Hardware Description, Goedel, Garbage Collected, Functional, Frontier, Fortran, Forth, Euphoria, Erlang, ElastiC, Eiffel, E, Dylan, DOS Batch, Directories, Declarative, Dataflow, Database, D, Curl, C-Sharp, Constraint, Concurrent, Component Pascal, Compiled, Comparison and Review, Cocoa, CobolScript, CLU, Clipper, Clean, Clarion, CHILL, Cecil, Caml, Blue, Bistro, Bigwig, BETA, Befunge, BASIC, Awk, Assembly, ASP, AppleScript, APL, Algol 88, Algol 60, Aleph, ADL, ABEL, ABC, or similar programming languages.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations,

elements, and/or components, but do not preclude or rule out the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

The process steps, method steps, algorithms or the like may be described in a sequential order, such processes, methods and algorithms may be configured to work in alternate orders. In other words, any sequence or order of steps that may be described does not necessarily indicate a requirement that the steps be performed in that order. The steps of processes described herein may be performed in any order practical. Further, some steps may be performed simultaneously, in parallel, or concurrently.

In addition to the embodiments and examples shown, numerous variants are possible, which may be obvious to a person skilled in the art relating to the aspects of the invention.

In an embodiment of the invention, the algorithm or logic or program or code associated with encryption systems and methods may be maintained in a device which is separate from the device or server in which the encryption systems and methods are enabled.

In an embodiment of the invention the systems and methods of the present invention can be used and made applicable for any online or network based activities such as but not limited to monetary transactions, online shopping, social networks, emails, chatting, on-line gaming sessions, messaging, multimedia-conferencing, application-sharing, e-voting, group-ware & collaboration, blogging, or any combination thereof.

In an embodiment of the invention, the algorithm used for encryption may have the following formula:

ALG = ALG1 (op1) ALG2 (op2) ALG3 .... (opN) ALGN+1 ,

where

ALG stands for an algorithm which may be a single set of instruction that may be enabled using a computer language

n= 1 to infinity

and

"op" stands for a functional operator including but not limited to logical operator or mathematical operator or comparative operator or string based operator, data and time operators.

In an embodiment of the invention, any action or process related to the systems and methods in accordance with the present invention, may execute entirely on a user's computing device, partly on a user's computing device, as a stand-alone software package, partly on a user's computing device and partly on a remote computing device or entirely on the remote computer or a server.

In an embodiment of the invention a user input is anything or any data or metadata provided by a user actively and with the users knowledge in the form of one or more alphabets or characters or any string or any computer program or any computer file.

In an embodiment of the invention, the systems and methods of the present invention may involve and provide methods to run self check, trouble shooting or program debugging.

A user is any person, machine or software that uses or accesses one or more of the systems or methods of the present invention. A user includes an automated computer program and a robot.

In an embodiment of the invention, the said code may have a combination of numeric or alphanumeric or symbolic characters used for protected and restricted access provided to a user to one or more digital systems or function or data, provided after necessary authentication or identification of the user.

In an embodiment of the invention, the encryption mechanism can be used by enabling a plugin or application or an icon or a bookmark on a website or a software or any graphical user input that is used for the systems and methods in accordance with the present invention.

In an embodiment of the invention, the encryption mechanism further comprises of one or more components which can be combined with one or more of other components of the mechanism in any combination, in an encrypted or unencrypted state, to generate an encryption key.

In an embodiment of the invention, the systems and methods can be practised using any electronic device. An electronic device for the purpose of this invention is selected from any device capable of processing or representing data to a user and providing access to a network or any system similar to the internet, wherein the electronic device may be selected from but not limited to, personal computers, mobile phones, laptops, palmtops, portable media players and personal digital assistants.

In an embodiment of the invention, the systems and methods of the present invention provides or enables a user interface which may allow commands for a command line interface and/or a graphical user interface (GUI) enabling a user to create, modify and delete data or metadata or program or logic or algorithm or parameters associated with encryption method or encryption program or encryption language.

In an embodiment of the invention, the system may involve software updates or software extensions or additional software applications.

In an embodiment of the invention, any form of internet security such as but not limited to, a firewall or antivirus or antimalware or registry protection can be used by a user in the same or different electronic device either simultaneously or separately, along with the systems or methods of the present invention.

In an embodiment of the invention, one or more user can be blocked or denied access or be required to reattempt access, to one or more of the aspects of the invention.
In an embodiment of the invention, a user may have a system to record or send alert or be informed in case any other user is accessing the user's electronic device remotely.

In an embodiment of the invention, the systems and methods of the invention may simultaneously involve more than one user or more than one data storage device or more than one host server or any combination thereof.

In an embodiment of the invention, the systems and methods of the present invention are used to prevent or restrict hacking or related phenomenon such as but not limited to phishing, man in the middle attack, inside jobs, rogue access points, back door access, use of viruses and worms, use of trojan horses, denial of service attack, sniffing, spoofing, ransomware or any combination thereof.

While this description has disclosed certain specific embodiments of the present invention for illustrative purposes, various modifications will be apparent to those skilled in the art which do not constitute departures from the spirit and scope of the invention as defined in the following claims, and it is to be distinctly understood that the foregoing descriptive matter is to be interpreted merely as illustrative of the invention and not as a limitation.

We claim,

1. A method for identifying an individual from an input image comprising the steps of:

a) preprocessing the input image by histogram equalization and Gaussian filtering;

b) generating a facial image by detecting a face from said input image;

c) rotating said generated facial image in such a way that eyes are in a horizontal line;

d) comparing said generated facial image with a database of saved facial images using normalized correlation technique;

e) generating a sorted list which comprises of facial images from said database having normalized coefficient of correlation greater than a threshold;

f) building a Gaussian scale space and difference of Gaussian images for all scales of said generated facial image and said facial images from said sorted list;

g) detecting keypoints with a local extrema in the difference of Gaussian images for all scales, assigning orientations to the keypoints and computing feature descriptors for the keypoints;

h) comparing the feature descriptors of said face with the feature descriptors of said facial images by calculating Eucledian distance;

i) selecting a facial image with minimum Euclidean distance as matched face.

2. A system for recognition of a face comprising:

1) at least one DSP processor that runs the method from 1.

2) at least one camera that captures the said input image

3) at least one display device which displays information about the said matched face.

Dated this 9th day of April 2013

Signature :-
Name : TALELE, Kiran

Signature :-
Name : BAIRATHI, Neha

Signature :-
Name : DAGA, Rahul

Signature :-
Name : DARJI, Jignesh

Signature :-
Name : PANDA, Rekha