IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (61-84)

Journal home page: www.ijreb.org

COMPRESSION TECHNIQUES APPLIED TOBIOMETRIC IMAGES AND THEIR TYPES - A REVIEW

***Abhilash.KS and **V.S.Dharun**

*Assistant professor (EC) Sarabhai Institute of Science & Technology Thiruvananthapuram

**Associate professor & Head Department of Biomedical Engineering, Noorul Islam University, Kumaracoil

ABSTRACT

There has been in depth analysis and numerous researches on image compression and storage. This paper gives a brief idea about biometric images, their different types, need for their recognition, a review of their formats, their storage space requirements and need for their compression along with different compression techniques and algorithms used for compression is presented. Based on this Review a general method for biometric Image Compression is recommended.

KEYWORDS: Biometric image, Image compression

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

1. INTRODUCTION

An image is an array, or a matrix, of square pixels arranged in columns and rows. Images may be black and white, color, 2-D, 3-D, high pixel, low pixel, etc. An image consists of a rectangular array of dots called pixels. The size of the image is given as width X height, in numbers of pixels. Resolution is usually measured in terms of DPI. [3] Though the images taken from a camera is in the analog form, for processing, transmitting and storage, images are to be converted in to digital form. Normally images in the digital format will be 2- Dimensional array of pixels. [2][3] General purpose Data Compression techniques or algorithms cannot be used for a compressing of image, as it is different from the digital data compression. [1].Different types of images are used in various applications like remote sensing, video processing, bio medical fields, biometric, satellite image techniques, etc.; which require compression for transmission and storage. There are different types of images as mentioned above. Now a day people go for computerized images as it is easy for compression and storage. In a (8-bit) gray scale image each picture element has an assigned intensity that ranges from 0 to 255. A grey scale image is what people normally call a black and white image, but the name emphasizes that such an image will also include many shades of grey. [2].

Figure 1: Each pixel has a value from 0 (black) to 255 (white). The possible range of the pixel values depend on the color depth of the image, here 8 bit = 256 tones or gray scales. [2].

1.1Biometric Image

The term "biometrics" is derived from the Greek words bio means life and metric means to measure. For us, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics which are unique to individuals hence can be used to verify or identify a person.[5] .Biometric imaging is a method used to identify a person; a security system has to compare their characteristics with a database. A scan of a person's iris, fingerprint, face, or other distinguishing feature is taken and a series of biometric points are drawn at key locations in the scan. In recent years, one of the most common forms of identification using camera [35], for people recognition has become common for security systems. For the successful

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

identification of an individual its require comparing an image of the individual to a database that contains the images of associative people. The main work is to compare each image in entirety, that is, point by point (pixel by pixel). This as we now is an extremely slow process, and quite expensive and in order to solve this problem, biometrics are used.

In biometrics, instead of compare the entire image, biometric points are placed at key locations, measurements between all the points are taken, and the results are compiled into a kind of score. [9] A score can be easily obtained from every image and then stored in the database. And when a new individual's image is collected, for a successful identification, all that is needed is to compile the score based on the image's biometrics, and quirky compare this new score to the scores in the database and to show the result according to the percentage of similarities of the new score with those in the database.[12] This is the main goal of a recognition system; that's when an image of an "unknown" person is given the algorithm finds a picture of the same person in a group of "known" or training images in the database[36]. It can identify images or videos of people automatically. It operates in two modes (1)Verification or authentication of individuals; that's compares a person's current image with a stored image of the person it wants to identify, as a result the system either confirms or denies the identity of the person. (2) ID or person recognition; compare the image of a stranger with the images of known persons in the database to determine their identity. [9]

The characteristic of a biometric imaging is biological or behavioral property of a person which can be measured and from which distinguished. Repeatable biometric features can be extracted for the purpose of automated recognition of individuals. The characteristic is captured with a capture device and are compared with a biometric sample representation of biometric characteristics. The biometric features are information extracted from biometric samples, which are used for comparison with a biometric reference .The aim of the extraction of biometric features from a biometric sample is to remove any superfluous information, which does not contribute to biometric recognition. This enables a fast comparison, an improved biometric performance, and may have privacy advantages. The main process in the biometric system is called enrolment. That is nothing but

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

the procedure involved in biometric imaging system; in order to recognize a person by their biometric characteristics and the derived biometric features, first of all a learning phase must take place. The enrolment data record comprises one or multiple biometric references and arbitrary non-biometric data such as a name or a personnel number. [3]From the recognition biometric score the biometric feature extraction creates biometric features, which are compared with one or multiple biometric templates from the biometric enrolment database. [3] As the biometric samples possess a statistical nature, no exact match is possible and as a result, the decision process will only assign the biometric data subject to a biometric template and confirm recognition if the comparison score exceeds an adjustable threshold. The system requires a shape or points measurement to compare against the information in the data base, in order to make an accurate comparison and determine if there is a match.[3][16]. Figure 2 represents a flow chart that represents the basic steps involved in an image processing [2] system.

1.2. Need for Biometric Image Recognition

Biometrics have been used to identify people, in one form or another for over a 100 years, as they relate to an individual's unique physical characteristics. They can never be forgotten, lost or copied, like a card or password and have been widely accepted as a fast, accurate and dependable way of confirming a person is who they say they are. A biometric system is effective until and unless it has the following four properties: (a) uniqueness, (b) invariance, (c) universality, and (d) resistance. It has even been developed into an App for smart phone users, proving that it is moving into our everyday lives.

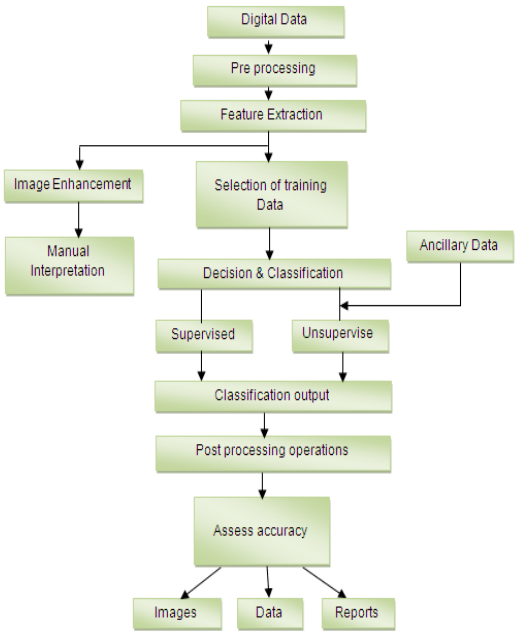

Figure 2: flow chart -steps involved in image processing.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' that is the user does not have to provide any information about the template to be used, or for 'negative recognition' of the person "where the system establishes whether the person is who he/she denies to be. The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective. As this all consumes much time, storage space and is much expensive for the saving of analog signals, we go for the biometric image processing. [2] [58] As we know the only method we can easily reduce space conception, time conception, etc.; is to go for digitalization of the data and so we go for image recognition in biometric techniques.

The two main stages in a biometric authentication system are: (i) Enrollment: to collect biometric data from a user and store it in the system, and (ii) Authentication: to identify or verify the identity of a user by matching the data provided by the user with the data stored in the system. Pattern Recognition, Machine Intelligence and Biometrics covers the most recent developments in Pattern Recognition and its applications, using artificial intelligence technologies within an increasingly critical field. It covers topics such as: image analysis and fingerprint recognition; facial expressions and emotions; handwriting and signatures; iris recognition [3][57]; hand-palm gestures; and multimodal based research. The applications span many fields, from engineering, scientific studies and experiments, to biomedical and diagnostic applications, to personal identification and homeland security.

1.3 Main biometric image recognition types:[6]

Fingerprint Recognition: Fingerprint recognition identifies people by using the impressions made by the minute ridge formations or patterns found on the fingertips. Finger printing takes an image of a person's fingertips and records its characteristics - whorls, arches, and loops are recorded along with patterns of ridges, furrows, and minutiae.[46] Information is processed as an

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

image and further encoded as a computer algorithm.

Face Recognition:A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source.

Iris Recognition: Iris recognition technology [7] [24] combines computer vision, pattern recognition, statistical inference, and optics. Its purpose is real-time, high confidence recognition of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance.

Hand Geometry Recognition: Hand geometry is a biometric approach to automatically recognize individuals based on the unique geometric features of hand.

Signature Recognition: A biometric identification method using a person's signature. Characteristics (writing speed, pen pressure, shape of loops, etc.) to identify that person.

Retina recognition: The pattern of blood vessels that emanate from the optic nerve and disperse throughout the retina depends on individuals and never changes. No two retinas are the same, even in identical twins.

Thermo grams: Thermo grams requires an infrared camera to detect the heat patterns of parts of the body that are unique to every human being (such as the face) . They are normally expensive because of the sensors

1.4. Most common biometric images and their common recognition algorithms

As we know the Biometric image recognition is a process that converts a high resolution scanned image into a required points or measurements. For the conversion of data's from analog to compressed images of digital signals we require an algorithm. The algorithm changes according to the type of source, data and need of type storage. The algorithm is the mathematical process used by the computer to perform the comparison of Biometric Technique. Let's go through the various algorithms for the different types of Biometric Imaging Technique.

(A) Iris image and its recognition

The technology of iris recognition is to provide accurate identity .Enrollment takes less than 2 minutes. Authentication takes less than 2

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

seconds. Although the terminology "iris-scanning" is often used, there is no scanning involved. Iris technology is based on pattern recognition and the pattern-capturing methodology is based on video camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual. An iris-recognition algorithm first has to localize the inner and outer boundaries of the iris pupil and limbs in an image of an eye.

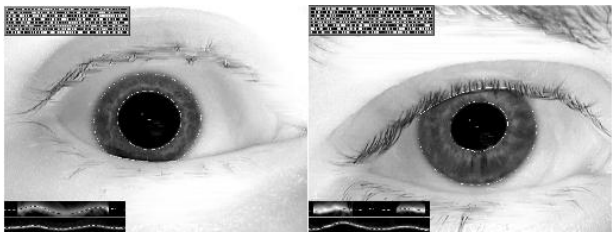

Figure3: Many irises have noncircular boundaries, creating problems for polar mappings. The box in the lower left of each image shows the inner and outer boundary curvature maps, which would be flat and straight if they were circles. Iris recognition has low failure rate. It uses features like furrows, ridges, coronas, crypt rings to characterize the sample

The algorithms used in iris Technique [55] [56] are Daugman's algorithm, the Boles's algorithm and the Arian's algorithm. The important algorithm used in iris biometric recognition [5] is Daugman's algorithms. Here Gabor wavelet transform is alsoused[32]. The result is a set of complex numbers that carry local amplitude and phase information about the iris pattern. In Daugman's algorithms, most amplitude information is discarded, and the 2048 bits representing an iris pattern consist of phase information [3]. Every Iris recognition algorithm consists of 3 main sections; these sections are as follow: 1. The image is preprocessed to detect and separate Iris from the whole image 2. Features representing the Iris patterns are extracted as a code 3. Decision is made by means of matching. [7]These cameras, the image capture process do not require bright illumination or close-up imaging. With a device activated by proximity sensor, a subject positioned 3" to 14" from the Enrollment Optional Unit is guided by a mirrored, audio-assisted interactive interface to allow an auto-focus camera to take a digital video of the iris. Individual images from the live video are captured using a frame grabber. The innovative algorithm of the iris recognition process analyzes the patterns in the iris that are

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

visible between the pupil and sclera and converts them into a 512-byte digital template. This value is stored in a database and communicated to Identification Control Units associated with portals where the subject has access privileges.

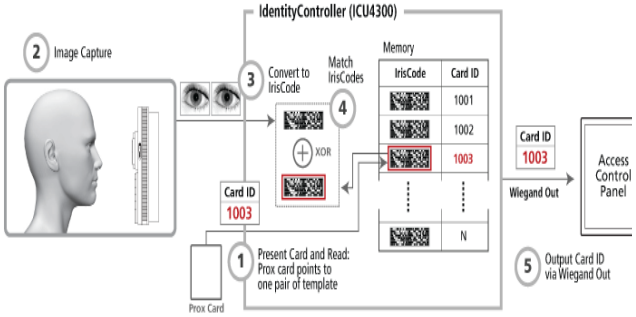

Figure4: - Block diagram of iris recognition technique in biometric image compression techniques.

(B) Fingerprint recognition

Many different algorithms exist: Direct correlation is practically not used, as it is not very efficient for large database. The general shape of the fingerprint is generally used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the finger print, and the presence of the core and the delta. Several categories have been defined in the Henry system: whorl, right loop, left loop, arch, and tented arch. Most algorithms uses minutiae, the specific points like ridges ending, bifurcation [3] [39]. Only the position and direction of these features are stored in the signature for further comparison. Some algorithms count the number of ridges between particular points, generally the minutiae, instead of the distances computed from the position. Pattern matching algorithms use the general shape of the ridges[4]. The fingerprint is divided into small sectors, and the ridge direction, phase and pitch are extracted and stored.

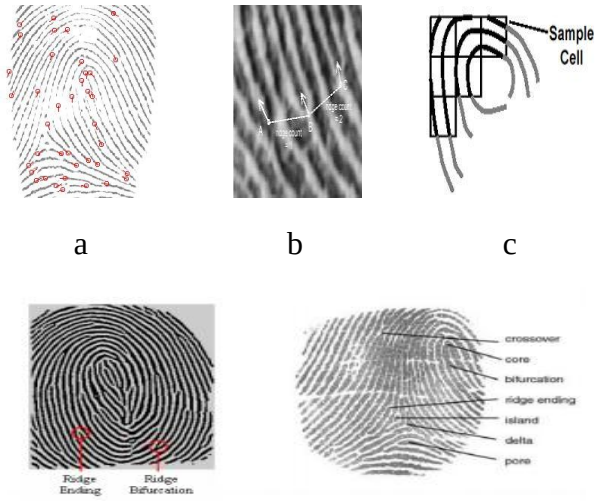

Figure 5: Different fingerprint algorithms, (b) minutiae, (c) ridge count, (d) pattern

A fingerprint usually appears as a series of dark lines that represents the high peaking portion of the friction ridge skin while the valleys appears as white space and are the low shallow portion of the friction ridge skin.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

Finger print identification is based primarily on location and direction of the ridge endings and splits along a ridge path. The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge. Bifurcations are points at which a single ridge splits into two ridges. Short ridges are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. The image below shows fingerprint features a) Two types of minutiae b) examples of other detailed characteristics sometimes used during the automatic classification and minutia extraction process.

The types of information that can collect from the fingerprint friction ridge impression include the flow of ridges. A minutia is the point where a ridge either terminates or bifurcates into two or more ridges and is defined in terms of x and y coordinates, and ridge orientation angle. Many sensor types- ultra sound capacitive thermal and optical are used for collecting digital image of a fingerprint. The main categories of the matching techniques for fingerprint are pattern matching and minutiae based matching.[48] Inked fingerprint impressions recorded on 38mm x 40mm (1.5"x1.6") areas of a fingerprint card are scanned and processed by an automated n fingerprint identification system (AFIS).[49] [47] Live-scan technology that relies on a moving light source and the principle of frustrated total internal reaction (FTIR) is used. Images captured by the live-scan reader can be directly inputted into an AFIS for subsequent processing. In this new technology elimination of ink, determination of image quality before recording, multiple copies of the same image from a single scanning, and the immediate creation of a file containing the electronic fingerprint image. Identification from fingerprints has two stage processes. The first is classification, which performs a coarse classification of fingerprints into one of five classes. The second one performs matching of details present in each fingerprint image. Fingerprints are easily being classified into one of five classes or types: arch, tented arch, left loop, right loop, and whorl. The four major approaches to automatic fingerprint classification. These are structural, syntactic, statistical, and the artificial neural network (ANN) approaches. The AFIS compares and matches the minutia between two fingerprints images and in the first step; the AFIS rotates

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

and translates the probe fingerprint into a standard position. After being rotated and translated, the similarity between probe and candidate fingerprints is a function of the geometric pattern of the minutia. The high score indicates a high probability of identification. To reduce file size, the JPEG algorithm has been used to compress the fingerprint images.

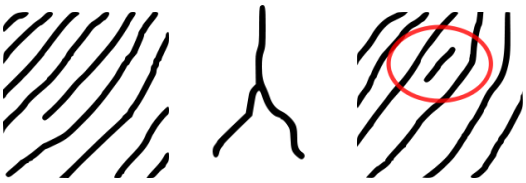

Figure 6: (a) Ridgeending (b) Bifurcation (c) Short Ridge

The FBI developed a different approach, based on wavelet technology. Rather than using an 8x8 pixel tile size, the wavelet scalar quantization (WSQ) algorithm globally compresses the image. This enables a compression ratio of 15:1 with minimal visual degradation in reconstructed images while we get only 8:1 compression ratio in 8x8 pixel tile. The new image capture devices capable of capturing finger ridge structures are based on CCDs, CMOS, capacitance, thermal effects, and electrical fields. Some readers scan pieces of the finger as it is swiped across a narrow window and then electronically sews the pieces back together.

(C) Face Recognition

Till 2006 the algorithms of Iris Biometric Technique was used by the Face Imaging Biometric Technique. After that a computer based algorithm was introduced successfully. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins. Some facial recognition algorithms identify facial features [20] [28] by extracting landmarks, or features, from an image of the subject's face. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.[50] [51] Recognition algorithms can be divided into two main approaches, geometric, which look at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

templates to eliminate variances. Facehas 80 nodal points and some of these points can be measured by software: Distance between eyes, width of the nose, Depth of the eye sockets, the shape of the cheekbones, the length of the jaw line By measuring these nodal points a special numeric code is created. This code is called a face print, and it is this code that represents the face in the database. Facial recognition technologies can be divided into two ways:

1. 2-d: it is the most ineffective way of biometrics. This method was mostly used in criminalistics. Now the computer version of this method appeared making it more reliable. This method does not need any expensive equipment, but reliability is very low. Method strongly depends on the light. Problems may occur if the person has glasses, beard, etc. Person should look straight to the camera, the expression of the face should be neutral.

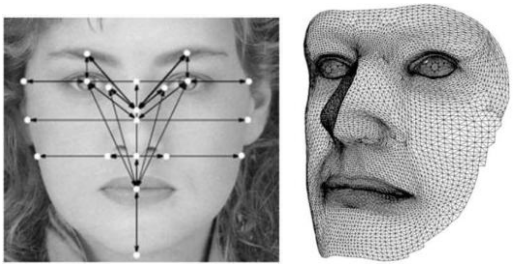

Figure 7. Example of 2-d and 3d technology 2. 3-D there is a lot of methods for3-D face recognition. These methods cannot be compared because all of them use different scanners and databases. The ad-vantage of this method is that there is no need for contact, the low sensitivity to such factors as: beard, glasses, another form of hair, colour of hair. Also 3D show high degree of reliability that can be compared with fingerprinting. But the negative side of the method is the expensive equipment; change of face expression reduces the statistical reliability of the method.[52] [53]

Between 2D and 3D methods there is so called transitional method which has the features of 2-D and 3D, realizes the information about the face. The method has better characteristics as 2D and also uses only one camera. The camera makes a picture of a person who looks directly at the camera, after this he turn his head and algorithm connect images together. The classical method of facial recognition is the creation of projection template of the face. First we project a face onto the elastic grid. Further, camera makes 10 photos in a second and these photos are worked up with the special program. The ray falls to the crooked surface starts bending. At the beginning visible light was used, but soon it was changed to the infra-red. At first stage the

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

program deletes all the photos where the face cannot be seen at all, or if there are some extra things. After this the 3D model of the face can be constructed. Beard, glasses and all other unnecessary things can be deleted. [29]The second stage is the analysis of the 3D model: different anthropometrical characteristics are found and constructed to the unique code.

Only a fully automatically recognition system can be implemented for a face recognition technique as it detects and identifies/verifies a face in an image or video sequence without human intervention. [31]Face recognition systems generally have two components, recognition and detection. Identification or verification of the face is done in the recognition component. The main requirement of this component is that the face be in a standard position. The component uses an algorithm on the bases of projection view-based. In a view-based algorithm, the face is represented as a set of two-dimensional images. [3] For different viewing conditions, the variations of a face are stored as separate individual image. In this projection-based algorithm, the image is projected onto a lower dimensional subspace, which is referred to as 'face space'. [54] It characterizes the differences among faces in a projection view-based algorithm as a set of points in face space. The identification between faces is measured by a similarity distance in face space and the similarity is analyses. At last the individual personal identification in the database is selected or identified to that of the minimal distance between the unknown face and the faces in the database. During verification the claimed identity will be accepted only if the similarity between the presented face and the claimed face lies within the set cut off value. The second component in face recognition method [3][95]is detection algorithm. Detection algorithms are used to either, detect and locate the face in "mug shot" [3] style images, or detect faces in images that contain multiple faces. In a mug shot style image, there is one face in the image and it occupies a majority of the pixels. Then a detection algorithm which is used to locate the face in the image is used to detect the set of facial features and a standard geometric configuration is formed from it. Detection method mainly detects and locates the eye and transforms face and checks that the eyes are on specified pixels. Both fully automatic face recognition systems and detection system together yields fully automatic face recognition technique. There are a number of techniques

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

developed for detection method. Among them neural networks-based and support vector machines based approaches are most common. The two basic classes in face recognition system are still and video. In video systems detection of the face are from a combination of motion, stereo, color, and facial pixel patterns. While a still image is restricted to color and facial pixel pattern, the face is detected, segmented, and passed to the recognition component. A set called the gallery is the set of known individuals in the data base is used for identification. An image of an unknown face presented to the algorithm is called a probe, and the collection of probes is called the probe set [3]. Other category of probes used is all frontal duplicates. A duplicate is an image taken in a different session or taken under special circumstances than the gallery image.

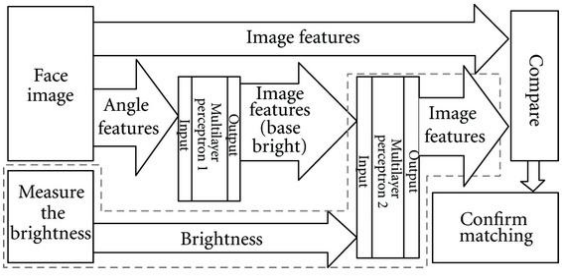

Figure8: Overall functional block diagram of face recognition biometric image compression technique.

In face recognition, performance is a function of the types of images in the gallery and probe set. For a number of identification scenarios, the output from the recognition system will be a list of the most similar individuals from the gallery to the probe. The main hurdle to the development of algorithms that can recognition faces in duplicate images is the availability of a large database of duplicates. The main advantage of faces is that they can be acquired non-intrusively.

2. Types of biometric images:

A. Tagged Image File Format (TIFF)

The TIFF [25][5] [20]is a particular image format in which the image is uncompressed but it is a flexible image format. Since no compression is used it is lossless and the image occupy larger space and not suitable for web transfer

B. Graphics Interchange Format (GIF)

GIF [3] [22] uses loss less compression.it can be used to store small biometric images simple graphics ,logos and cartoon style images etc. can be applied for images having colors less than 2^8, ,grayscale.GIF is usually limited to an 8 bit colors.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

C. RAW

Direct Digital cameras images constitute RAW [3][22]file format. It can be either loss less or lossy compression type. The main Disadvantage of RAW Images are that they are unstandardized images differs with manufactures. Usually these images require software's from manufacture's toview.

D. Portable Network Graphics (PNG)

The PNG [5] [20][26] supports 8 bit, 24 bit, 48 bit true color with and without alpha channel file formats. Lossless PNG format is advanced and is best in comparison with JPEG which is lossy. PNG file is 10% to 30% more compressed than in a GIF format. The main advantage of this format is that it is able to achieve smaller size with more colors.

E. Joint Photographic Expert Group (JPEG)

JPEG [5] [20] is used for storing 24 bit photographic images in lossy compression format. It is mostly used in multimedia and imaging industries. JPEG is 24 bit color format having millions of colors and more superior comparison. It is used for VGA (video graphics Array) displays.JPEG uses lossy compression to support 8 bit gray scale image and 24 bit color images.

F. JPEG2000

JPEG 2000 [5] [20] is a new compression standard which can be used for lossless and lossy storage.JPEG2000is used to improve the JPEG format.

G. Exchangeable Image File Format (Exif)

The Exif [5] [28] is having same properties to JFIF format with TIFF extension. It is used to exchange and record of images .usually the exchange is carried out with image metadata between the digital camera and editing and viewing software.

H. WEBP

A new image format that use lossy compression isWEBP. [5] [22]Google designed it to reduce image file size and to increase the speed when web page is being loaded. VP8s infraframe coding is its base.

I.Bitmap (BMP)

Microsoft windows OS related graphic file are dealt with Bitmap (BMP) [5] [28][33] file format. These files are usually uncompressed and are large. Mainly used in basic windows programming. BMP images are binary files and do not supports true colors.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

J. NETPBM

Three family formats are included in NetPbm format [5] [20]: they are the PPM (portable Pixel Map), the PGM (portable Gray Map) and the Portable bit map [34]. They are pure ASCII files or raw binary files.

2.1 Need for compression of Biometric Images

Image compression addresses the problem of reducing the amount of data required to represent a digital image. [3] It is a process intended to yield a compact representation of an image, thereby reducing the image storage/transmission requirements. Table below shows the comparative size from normal text to high compressed image. Examples given in Table clearly show need for sufficient storage space and more bandwidth because long transmission time is required for uncompressed image. So the only one solution is to compress the image. [1]. Image compression is applied to reduce the number of bits which represent the image we use different lossless and lossy compression algorithms [5] on the various biometric sample data. Mainly, we relate the application flossless JPEG, JPEG-LS, lossless JPEG2000 and SPIHT, PNG, GIF and a few general purpose compressions chemes to imagery of the following biometric modalities: finger print, iris, retina, face and hand. When the increasing usage of biometric systems gets increased day by day, the question arises naturally how to store and handle the acquired sensor data. The compression of these data may become imperative under certain circumstances due to the large amounts of data involved.

DATA	IMAGE SIZE	NO OF BITS/PIXELS	UNCOMPRESSED SIZE	TRANSMISSION BANDWIDTH	TRANSMISSION time
PAGE	11"X9"	Resolution depentant	6 kB	33KBPS	1-3 SEC
CAMERA IMAGE	800X600	8BPP	1.5 -2 MB	100MBPS	50 MIN
COLOUR IMAGE	512X512	24BPP	786kB – 1 MB	8MBPS	5MIN
BIOMETRIC IMAGE	2048X1680	12BPP	3MB - 5MB	200MBPS	90MIN

Table: Different Uncompressed Images and its storage space

Among other possibilities, like compressed template storage on IC cards, compression technology may be applied to sample data in two stages of the processing chain in classical biometric recognition. A significant amount of work exists on using compression schemes in biometric systems. Principle of compression is given as digital image is basically array of various pixel values and a correlation exists between Pixels of neighbourhood so that these pixels contain redundant bits. [3] [25] Redundant bits are removed from the image by using the compression algorithm so that there is

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

reduction in image size and the image is compressed. Two main Components of Image compression are: 1) redundancy reduction and 2) irrelevant data reduction. Extra bits or repeated bits are removed to achieve Redundancy reduction. In irrelevant reduction the less important information is omitted. There are three types of redundancies. They are 1) Coding redundancy, 2) Inter pixel redundancy and 3) Psycho visual Redundancy. Correlated pixels of an image leads to Inter pixel redundancy .When less number of code words required instead of larger symbol the Coding redundancy is present. In psycho visual redundancy data is ignored by the normal visual system. [1].

2.2 Performance parameters

In order to measure the performance of the image compression algorithms two performance parameters are used. 1. PSNR (peak signal to noise ratio) 2. Mean square error (MSE). The peak error between the compressed image and original image is measured in terms of PSNR. The higher value of PSNR indicates higher quality of image. To calculate PSNR, MSE is first computed. Cumulative difference between the compressed image and original image is MSE. Small value of MSE improves image quality and reduces the error.

$$\mathbf{MSE= \sum_{M,N}[I_1(m,n) - I_2(m,n)]^2 / M*N}$$

M &*N* - number of rows and columns in the input images. PSNR is computed from below equation

$$\mathbf{PSNR = 10 \log_{10} [R^2 / MSE]}$$

2.3 COMPRESSION ALGORITHMS

Lossless and Lossy compression [11] [13][14] are two types of compression algorithms. In the loss less compression the compressed image is totally replica of the original input image, there is not any amount of loss present in the image. While in Lossy compression there is some amount of loss and the compressed image is different from the input image [8].

A. Lossless compression Techniques

The reconstructed image is same to the input image in lossless compression scheme. In this scheme the image is first converted into image pixels each single pixel is then processed. Next image pixel value is predicted from the neighbourhood pixel .the final step is using different encoding method coding of the difference between the predicted value and actual intensity of next pixel is performed.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

Lossless compression encoding and decoding methods are as below

1. RLE (run length encoding): In this simple image compression technique [2][17][34] in which sequence of identical symbols are replaced by a pair containing the symbol and length at which the number is repeated. For fax standardization it is used.

2. Statistical Coding: The techniques are included in Statistical Coding. 1. Huffman Encoding, 2. Arithmetic Encoding 3. LZE Encoding.[37][39]

3. Huffman Encoding: by removing irrelevant information the file size is reduced from 10-50%the pixel values which occur frequently is given a smaller bit code and repeated pixel value is given to higher bit code. The encoding procedure using Huffman coding is as follows. The input images are first divided into 8x8 blocks, and then a particular symbol is given to each block. Each block is then applied with Huffman code to encode all block is done

4. Arithmetic Encoding: Rissanen introduced this encoding technique .In this technique encoding and decoding of last symbol is first done [40]. the principle of arithmetic encoding is infinite value for symbol alphabet is not acceptable the finite value for all possible symbol sequence of given length is not accepted, for any given input sequence of symbols, the real number in the interval [1,0]can assign a unique subinterval.

5. LZW coding: coding is based on a dictionary and dictionary is fixed during encoding and decoding for static dictionary coding. Coding of dictionary is updated with the introduction of new word in dynamic dictionary coding.

6. Area coding: RLE's enhanced version is area coding .Better compression ratio can be achieved using area coding .it is highly effective and can be limited to application of nonlinear transformation.

B. Lossy Compression Techniques

Provides higher compression ratio in comparison with lossless compression. Some amount of information is lost as a result there is difference between compressed image and original image.

1. Transform Coding: in this original image is portioned into small blocks of smaller size based on the transformation used coefficients are obtained for each block examples are wavelet and curve let. The output

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

is obtained by computing resulting coefficients by using quantization technique, the final output is taken from quantize which uses symbol encoding technique then image is reconstructed by reverse process at the decoder.

2. Block Truncation coding: the input image is portioned into non overlapping blocks of pixels. The mean of pixel value is calculated by quantize for all non-overlapping blocks. The process of thresholding sets the image pixels to zero or one. The reconstructed value is obtained for each segment in the bit map. Greater compression ratio can be obtained for larger block size but at cost of image quality

3. Sub –band Coding: Finds application in speech and image coding. The frequency bands of the signal are split and the coding of sub band is done by encoder. The sub band signals are decoded unsampled and passed through synthesis filter at the decoder .the compressed image is obtained by properly summing the sub band coefficients [43].

4. Vector quantization: scalar quantization technique when extended in multiple dimensions resulted in vector quantization. It consists of dictionary of fixed size vectors called code vectors. Non overlapping blocks called image vectors are formed by partitioning of given image. Closest matching vector in dictionary is determined and its index in dictionary is determined and is used as encoding of original image vector for each input image vector. Vector quantization technique finds its application in multimedia as it has fast lookup capability at decoder side[45].

3. CONCLUSION

Here all the major biometric image recognition types have been discussed in detail along with their algorithm .from all above discussed detailed biometric recognition it is evident that biometrics influenced area of monitoring, remote surveillance , access control and verify transactions executed via ecommerce and high class security systems. In above discussed area problems of authentication and identification have been discussed in detail .the storage space requirement for the biometric images has been analyzed and is presented. After considering the storage requirement a study of image compression techniques and algorithm is presented and as a conclusion new and new techniques are developing which offer better compression ratios. Based on the review we reached into conclusion that the compression

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

algorithm used for biometric images depends on image quality, amount of compression, and speed of compression.

4. REFERENCES

[1] Mr.Chandresh k parmar, prof.Kruti pancholi, "a review on image compression techniques", issn: 0975 – 6736| nov 12 to oct 13 | volume – 02, issue – 02

[2] Introduction to image processing, www.hubblesite.org/sci.d.tech/behind_the_pictures/http://heritage.stsci.edu/commonpages/infoindex/ourimages/color_comp.html

[3] Wikipedia links http:/ /en.wikipedia.org/wiki/Biometrics,http:// en.wikipedia.org/wiki/Biometric_points# Biometric_points_or_shapes, http://en.wikipedia.org/wiki/Iris_recognition http:// en. wikipedia.org/ wiki/Facial_recognition_system# Software

[4] A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In Proceedings of Second International Conference on Biometrics, pages 760–769, Seoul, South Korea, August 2007.

[5] Dr. MariosSavvides, "Introduction to Biometric Recognition Technologies and Applications", http://www.biometricscatalog.org/biometrics/biometrics_101.pdf or biometrics_101.pdf, www.cylab.cmu.edu

[6] Parvinder S. Sandhu, Iqbaldeep Kaur, Amit Verma, Shailendra Singh , "Biometric Methods and Implementation of Algorithms", International Journal of Electrical and Electronics Engineering 3:8 2009

[7] Ameer A. Mohammed Baqer, Suhas H. Patil, "Efficient Iris Biometrics Technique for Secure Distributed Systems", International Journal of Digital Society (IJDS), Volume 3, Issue 1, March 2012

[8] Sonal, Dinesh Kumar, "A STUDY OF VARIOUS IMAGE COMPRESSION TECHNIQUES"

[9] Subramanya A, "Image Compression Technique," Potentials IEEE, Vol. 20, Issue 1, pp 19-23, Feb- 2001

[10] Woods, R. C. 2008. Digital Image processing.New Delhi: Pearson Pentice Hall, 3 Edition,, Pages 1-904..

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

[11] Hong Zhang, Xiaofei Zhang & Shun Cao, " Analysis & Evaluation of Some Image Compression Techniques," High Performance Computing in Asia Pacific Region, 2000 Proceedings, 4th Int. Conference, vol. 2, pp 799-803,14-17 May, 2000

[12] Ming Yang &NikolaosBourbakis ,"An Overview of Lossless Digital Image Compression Techniques," Circuits & Systems, 2005 48th Midwest Symposium ,vol. 2 IEEE ,pp 1099-1102,7 – 10 Aug, 2005

[13] Milos Klima, KarelFliegel, "Image Compression Techniques in the field of security Technology: Examples and Discussion,"Security Technology, 2004, 38th Annual 2004 Intn. Carnahan Conference, pp 278-284,11-14 Oct., 2004

[14] Ismail Avcibas, Nasir Memon, BulentSankur, Khalid Sayood, " A Progressive Lossless / Near Lossless Image Compression Algorithm,"IEEE Signal Processing Letters, vol. 9, No. 10, pp 312-314, Oct022

[15] [3] http://en.wikipedia.org/wiki/Image_file_formats

[16] WenShiung Chen, en- HuiYang& Zhen Zhang, " A New Efficient Image Compression Technique with Index-Matching Vector Quantization," Consumer Electronics, IEEE Transactions, Vol. 43, Issue 2, pp 173-182, May 1997.

[17] David H. Kil and FancesBongjoo Shin, " Reduced Dimension Image Compression And its Applications,"Image Processing, 1995, Proceedings, International Conference,Vol. 3 , pp 500-503, 23-26 Oct.,1995

[18] C.K. Li and H.Yuen, "A High Performance Image Compression Technique For Multimedia Applications," IEEE Transactions on Consumer Electronics, Vol. 42, no. 2, pp 239-243, 2 May 1996.

[19] Shi-Fei Ding, Feng-Xiang Jin, " Information Feature Analysis and Improved Algorithm of PCA," Proceedings of the 4th International Conference on Machine Learning and Cybernetics, Guangzhou, pp 1756-1761 , 18-21 August,2005

[20] Vo Dinh Minh Nhat, Sung Young Lee, "Two-Dimensional Weighted PCA

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

algorithm for Face Recognition," Proceedings 2005 IEEE International Symposium on Computational Intelligence in Robotics and Automation, pp 219-223, June 27 2005

[21] A Survey of Unimodal Biometric Methods NimalanSolayappan and ShahramLatifi Department of Electrical engineering, University of Nevada at Las Vegas, USA

[22] A SURVEY OF BIOMETRIC RECOGNITION METHODS KresimirDelac , MislavGrgic HT - Croatian Telecom, Carrier Services Department, Kupska , Zagreb, CROATIA University of Zagreb, FER, Unska 3/XII, Zagreb, CROATIA, 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia184,

[23] Natalia A. Schmid, Joseph A.O'Sullivan,"Performance Prediction Methodology for Biometric Systems using a Large Deviations Approch", IEEE Transaction of Signal Processing, October 2004.

[24] Li Ma , Tieniu Tan , Yunhong Wang , Dexin Zhang , " Personal Identification Based on Iris Texture Analysis" , IEEE Transactions on Pattern Analysis and Machine Intelligensce , Vol. 25 No. 12, December 2003.

[25] Keshab K. Parhi, Takao Nishitan; "Digital Signal processing for multimedia systems", ISBN0-8247-1924

[26] A Survey of Unimodal Biometric Methods NimalanSolayappan and ShahramLatifi Department of EE, University of Nevada at Las Vegas, USA

[27] Understanding Image Types"http://www.contentdm.com/USC/ tutorial/i mage-filetypes.pdf.1997 2005,DiMeMa,Inc,Unpublished..

[28] R. Chellappa, C. L. Wilson, and S. Sirohey. Human and Machine Recognition of Faces: A Survey. Proceedings of the IEEE, 83(5), 1995.

[29] E. Hjelmås and J. Wroldsen. Recognizing Faces from the Eyes Only. In the 11th Scandinavian Conference on Image Analysis, 1999. International Journal of Electrical and Electronics Engineering 3:8 2009 496

[30] M. Lades, J. C. Vorbrüggen, von der Malsburg, R. P. Würtz, andW. Konen. Distortion Invariant Object Recognition in the Dynamic Link Architecture. IEEE Transactions on Computers, 42(3), 1993.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

[31] B. S. Manjunath, R. Chellappa, and C. von der Malsburg. A Feature Based Approach to Face Recogntion. In Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1992.

[32] Coding Facial Expressions with GaborWavelets Michael Lyons and Shigeru Akamatsu ATR Human Information Processing Research Laboratory 2-2, Kyoto 619-02, Japan Kyushu University Proceedings, Third IEEE International Conference on Automatic Face and Gesture Recognition, April 14-16 1998, Nara Japan, IEEE Computer Society, pp. 200-205.

[33] John Miano; "Compressed image file formats: JPEG, PNG, GIL,XBM,BMP,Edi-2,January-2000, page 23.

[34] Majid Rabbani, Paul W.Jones; "Digital Image Compression Techniques". Edition-4, 1991.page51.

[35] A. Adler. Vulnerabilities in Biometric Encryption Systems. In Proceedings of 5TH International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), volume 3546, pages 1100–1109, Rye Brook, USA, 2005.50

[36] A. Adler, R. Youmaran, and S. Loyka. Towards a Measure of Biometric Information. Pattern Analysis and Applications, 2008.

[37] Ronald G. Driggers; "Encylopedia of optical engineering", Volume 2, Edition 1,2003.

[38] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni. Fake Finger Detection by Skin Distortion Analysis. IEEE Transactions on Information Forensics and Security, 1(3):360–373, September 2006.

[39] Ioannis Pitas; "Digital image processing algorithms and applications.", ISBN 0-471- 37739-2

[40] A.S. Ragab, Abdalla S.A. Mohmed, M.S. Hamid,"Efficiency of Analytical Transforms for Image Compression" 15th National Radio Science

[41] BCC Research. The Global Biometrics Market, 2007. http://www.bccresearch.com/report/IFT042B.html.

[42] A. Bertillon. Identification Anthropometrique: Instructions Signaletiques. Melun: Imprimerie Administrative, 1893.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

[43] Rafael C. Gonzalez, Richard Eugene; "Digital image processing", Edition 3, 2008, page 466.Alan Conrad Bovik; "Handbook of image and video processing", Edition 2 1005, page 673

[44] G. Bleumer. Multilaterial Security in Communications, chapter Biometric Authentication and Multilateral Security. Addison-Wesley, 1999.

[45] Deke McClelland, Galen Fott; "Photoshop elements3 fordummies" Edition 1, 2002, page 126.

[46] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint Image Reconstruction From Standard Templates. IEEE Transactions on Pattern Analysis and MachineIntelligence, 29(9):1489–1503, 2007.

[47] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn. Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault. In Proceedings of Conference on Information Security and Cryptology, pages 358–369, Beijing, China, December 2005.

[48] T. Clancy, D. Lin, and N. Kiyavash. Secure Smartcard-Based Fingerprint Authentication. In Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications, pages 45–52, Berkley, USA, Nov 2003.

[49] E. C. Chang and S. Roy. Robust Extraction of Secret Bits From Minutiae. In Proceedings of Second International Conference on Biometrics, pages 750–759, Seoul, South Korea, August 2007.

[50] D. Colbry. Human Face Verification by Robust 3D Surface Alignment . PhD thesis, Department of Computer Science and Engineering, Michigan State University, June2006.

[51] Y. C. Feng and P. C. Yuen. Protecting Face Biometric Data on Smartcard with Reed-Solomon Code. In Proceedings of CVPR Workshop on Biometrics, page 29, New York, USA, June 2006

[52] E. J. C. Kelkboom, B. Gkberk, T. A. M. Kevenaar, A. H. M. Akkermans, and M. van der Veen. "3D Face": Biometric Template Protection for 3D Face Recognition. In Proceedings of Second International Conference on Biometrics, pages 566–573,Seoul, South Korea, August 2007.

[53] K. Kollreider, H. Fronthaler, and J. Bigun. Evaluating Liveness by Face Images and the Structure Tensor. In Proceedings of Fourth IEEE Workshop

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (61-84)
IJREB
Journal home page: www.ijreb.org

on Automatic Identification Advanced Technologies, pages 75–80, Buffalo, USA, October 2005.

[54] G. Littlewort, M. S. Bartlett, I. Fasel, J. Susskind, and J. Movellan. Dynamics of facial expression extracted automatically from video. In IEEE CVPR, (Workshop on Face Processing in Video), 2004.

[55] E. C. Lee, K. R. Park, and J. Kim. Fake Iris Detection by Using Purkinje Image.In Proceedings of International Conference on Biometrics, volume LNCS 3832, pages 397–403, Hong Kong, China, 2006.

[56] J-E. Lee, A. K. Jain, and R. Jin. Scars, Marks and Tattoos (SMT): Soft Biometric for Suspect and Victim Identification. In Proceedings of Biometric Consortium Conference (BCC), Tampa, Florida, September 2008.

[57] J. Daugman. Recognizing Persons by their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in Networked Society, pages 103–122. Kluwer Academic Publishers, London, UK, 1999.

[58] J. Flusser and T. Suk. Rotation Moment Invariants for Recognition of Symmetric Objects. IEEE Transactions on Image Processing, 15(12):3784–3790, 2006