



Article

Fake Biometric Detection Based on Image Quality Assessment Application to Iris Face & Fingerprint

Sarah Kareem Salim^{1*}

1. Electrical Engineering Department, University of Misan, Misan 62001, Iraq

* Correspondence: sarahalthahabi@uomisan.edu.iq

Abstract: Biometric is a technological system that utilises the data for an individual to distinguish it. This technology stores particular information for one of the kinds of organic properties to operate in a workable way. It can be utilized in biometric frameworks by government, organizations, and associations for security reasons. An airplane terminal checking gadget, a "bio-secret key" framework are examples of a biometric system utilizations of the recognizing information for a security result. Be that as it may, we require security for this data and also verification of that individual. This novel software-based technology help to look at the data of an individual is genuine or counterfeit because of that the last aftereffect of validation can be got. Therefore, the major aim of this piece of work is to improve the well-being of the biometric acknowledgement system that includes image quality evaluation to make fast, simple to comprehend and minimal effort. Three applications of data were utilised here which are fingerprint, iris, and face detection. The proposed approach uses features of overall image quality derived from a single image to differentiate with both true and fake samples. It gives efficient protection against different spoofing attacks.

Keywords: Image quality assessment, biometrics, security, attacks, countermeasures.

1. Introduction

The biometric framework is a computer framework which is utilized to investigate human characteristics. The biometric framework comprises detecting, matching modules, and feature extraction. This approach introduces a multi-biometric system. Using Image Quality Assessment, we shield the biometric framework from counterfeit attacks. The term Biometric system related to technology. It will be dealing with human characteristics:

A. Physiological characteristics

The body parts will describe the Physiological features, e.g., iris, fingerprint, face, etc. Fingerprint Recognition: Every fingerprint of every individual unique, even twins have different fingerprints. Identification of fingerprints is by far the most accepted technique of biometric recognition. Fingerprints were being used to distinguish between people for a long time. Recognition of Iris: A computerized biometric strategy for identification makes use peoples' eyes irises; whose random patterns are different and could be differentiated from a distance. Iris is the colour ring surrounding the pupil of every person. Every person has a unique iris. Face Recognition: which is the system that distinguishes between the face and its background. It is most effective if a face within an audience must be recognized by the framework. The framework after this examines the characteristics of the person's face-their main highlights and the terrains and landmarks of his face and treats them as references and compares them to those stored in the system database.

Citation: Sarah Kareem Salim. Fake Biometric Detection Based on Image Quality Assessment Application to Iris Face & Fingerprint. Vital Annex: International Journal of Novel Research in Advanced Sciences 2024, 3(3), 72-87.

Received: 10th July 2024Revised: 11th July 2024Accepted: 24th July 2024Published: 27th July 2024

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

B. Behavioural characteristics

Characteristics of behaviour are associated with the individual's behaviour, for example, voice, signature, keystroke, and so on. The biometric framework separates in detecting, feature extraction, and matching modules.

C. Liveness detection methods

Generally, these methods are categorized into each of 2 groups. (i) Hardware-based techniques: This approach works by attaching the sensor to a specific component to recognize particular characteristics of a living object, like blood pressure, fingerprint sweat, or clear eye reflections. (ii) Software-based techniques: For this situation the falsified attribute is spotted once it has been gathered with a regular sensor, i.e. features used to define real and false attributes are derived from the biometric sample rather than the object itself.

These two techniques will give each other a few advantages and disadvantages and, generally, the combination of both may be the most effective security technique for through the biometric systems safety. Hardware-based strategies typically implement a greater falsified rate of recognition as a coarse contrast, whereas software-based schemes generally cost lower than hardware-based because there is no need for an additional device, but far less demanding as the consumer is straightforward in their application. Besides that, since they straightly can work at the gathered sample, not on the biometric attribute on its own. Software-based schemes can be incorporated into the function extractor module, which allows them ready to detect certain forms of illegitimate break-in tries that are not generally known as spoofing attacks [3].

Literature Review

In 2010, J. Galbally, C Mcool, J. fierres the face variety framework with the slope climbing algorithm, for that slope climbing calculation is utilized. In that calculation is legitimate thinks about and streamline information, which gives the consequence of an 85% achievement rate. Rather than utilizing individual distinguishing proof like numerical passwords, designs we utilize the biometric framework. Utilizing the computation of the Bayesian incline climbing, the method is led between the circuitous attack and the measurement matcher parameter. It analyzes roundabout assault and gives a score by matcher, so this calculation is created to use genuine people data. The value of this framework is, it will think about every single outcome, so there is no probability of missing the test. Consequently, the proficient outcome is taken at yield. The disadvantage of that system is the handling of calculation requires some time.

In 2016, Sarvesh Manav Meena, Prof. Arun B. Nandurbarkar proposed a liveness evaluation at multimodal biometrics through the picture quality appraisal. In that picture quality parameters are utilized to separate genuine and fake pictures. The picture quality appraisal having two sections initially is subjective part, in that information is contrasted and positioning of parameters after that outcome is shown in five classes of extremely poor, poor, great, great, and magnificent. And afterwards, this procedure aims to offer placement to test if the most severe element matches a different view, then provides a brilliant rank or if there are lesser matches between the information and the special example, it provides the reference implementation an extremely poor rank. Another is objective, which comprises two pictures one is a reference, and another is test pictures. It expresses some writing review on paper as it takes after 1) "Iris liveness discovery given value related highlights", by J. Galbally, J. Fierrezin 2012 proposed picture quality-related parameters which are programming-based answer for iris recognition. Iris can be distinguished a few properties like concentration, impediment (which identify the structure of eyelashes). 2)"Universal picture quality record", by Zhou Wang proposed a new all-inclusive picture quality list which is anything but difficult to material different picture preparing the application. It comprises parameters like loss of connection (It

measures the level of straight relationship between X and Y) and luminance blending. The preferences are minimal effort and quick reaction.

In 2014 J Galbally, Sebastian marcells, inquire about a quality appraisal for counterfeit biometric identification: application to iris, unique impression of the finger, and face acknowledgment by utilizing 25 picture characteristics are looked over one picture. Those characteristics are contrasting and a counterfeit picture or testing picture. The parameter depends on full reference and no reference. It utilizes MATLAB programming. This framework is having multitasks and multi-biometric insurance techniques. This paper utilizes the general picture quality parameter to recognize genuine and counterfeit examples. With the assistance of picture quality evaluation, the distinctive highlights are motivated to contrast with distinguishing unique examples. Its ways to deal with make activity quick, not destructive, easy to use.

In 2015, Yujia Jiang & Xin Liu proposed a fake unique finger impression identification given co-event grids. In this paper co-event framework or novel programming is for the most part utilized. It comprises falsely counterfeit unique marks made utilizing a material like gelatin or silicon. It is having diverse strategies like sweat pores-based technique, sweat based strategy, skin flexibility technique, and surface strategy. It likewise has a highlight extraction process, in which preparing strategy (used to make a judgment) another is trying procedure (for a look at the picture). In the include extraction, picture pixel esteems are right off the bat quantized. Quantization activity will cause loss of data this is the weakness of this task.

In 2015, S Chinthu, C Dhanabal proposed counterfeit distinguishing proof in the finger, iris, and face utilizing appraisal of picture quality. In that novel programming is utilized to catch unique pictures to improve quality. Catch pictures are imprinted on paper utilizing a business printer, accessible at the sensor. By utilizing this, the framework handles distinctive sorts of assaults and giving abnormal state assurance. Framework engineering comprises diverse modules for a location like liveness recognition and assault on the biometric distinguishing proof framework. The assault on a framework like unique pictures is caught for better quality, imprinted on pares used for the business printer. Utilizing this data or printed pictures displayed on the sensor of the biometric framework this framework is catch and contrast by programming and diverse parameters and identify the framework that data is genuine. This framework uses distinctive techniques like histogram leveling (modifying picture forces to improve differentiate), diminishing pictures (it is the change of an advanced picture into a streamlined), multi-point recognition, and execution measure. By breaking down this parameter the last discovery result is made. It gives an abnormal state of security over various sorts of assaults. For parameter examination, it needs a high caliber of the picture.

In 2015, Tija Thomas, Helice K Babu, Ambikadevi Amma T. proposed a novel fake identification framework for biometric modalities. By utilizing novel programming multi-biometric counterfeit identification, we get a genuine and counterfeit examination. It comprises picture quality evaluation having full reference use to test, and no reference database data isn't utilized. Exploring a collection of different highlights was the main part of procedure, A rational classifier will be provided that provides the likelihood of images. A novel parameterisation that use 30 general measures of image quality is taken into account in these 30 proposed frameworks. This framework utilizes just a piece of single information, a biometric check to be called genuine or counterfeit with a clear end goal to ensure its rationalization and efficacy. This strategy considers the entire picture as opposed to considering any attributes particular properties, no preparing steps are done preceding the figuring of IQ highlights. In the wake of registering all highlights, it will be a diminished figuring load. The fundamental highlights are chosen to utilize principle component analysis (PCA). Because of this, it is quick and easy to use.

In 2015, Aleena T. A, Chithrak, R. Ramachanran proposed security for the biometric framework. In that Gaussian separating is utilized with Fourier change. The proposed framework demonstrates it can be performing a multilevel task while looking at gadgets then it gives 90% of accurate result is from the biometric framework. By using extricated picture quality measures, the input picture is named genuine or counterfeit. use of full reference of database data contained in it to be analyzed, no reference (database data is missing, some methods are being used), methodological approaches to bending, JPEG quality file and High-Low incidence file are two distinct disfigurement features that are delicate to photo sharpness, arrangement-based method, display ready to use clean and invalid images and characteristic static strategy to scene group recognized data with Gaussian channel1. It turns out to be a proficient security upgrading innovation for the biometric framework.

In 2015, Anju. M. I, G. Sheeba, G. Sivakami proposed a multimodal biometric acknowledgment security framework, with various calculations. Additionally, it comprises the best biometric framework contrasting given data as far as precision, time, or highlight extraction. The consolidated technique will lessen preparing time and increment proficiency. The security and verification of people are vital for various parts of our lives. The vast majority having confirmation their personality on everyday bases incorporate ATM secured to ID cards and passwords to conquer a considerable lot of the shortfalls of this technique, it recognizes an individual based their identity as opposed to what they are recollected. Improving the well-being of biometric recognition methods is the aim of the suggested system through the inclusion of liveness assessments. These ways to deal with various calculations for iris, unique mark, and face acknowledgment.

In 2012, Maria Martini a picture quality appraisal in light of edge conservation. For Picture pressure, the transmission edge discovery technique is utilized. It precisely speaks to the subjective nature of proposed pictures that are signed for the plan and appraisal of a picture pressure. It is critical to figure the nature of getting pictures with the least reference to the transmitted one. For the transmission framework, picture quality measures can be assessed at collectors and gave as criticism data to a implementation Controller on the aimed quality metric info side which require no reference or needs the least reference to a unique image. Human eye understanding is extremely precise to edge and the image's design of data supports the proposal of a lower reference quality metric. Determination of Sobel filtering brings about low many-sided quality metric, have high estimation speed, and give continuous execution. The impediment of this framework is the lower limit estimations causes to higher affectability to edge. The high appraisal of the limit are too small, considerable components of the image are viewed as edges which are unimportant for quality assessment.

Mojtaba Sepasian, Wamadeva proposed for helping to identify ridiculing assaults related to unique marks. It guarantees the input picture of the finger is genuine or fake. There is equipment and additionally, programming procedures are utilized to distinguish parodying assault, likewise, they say willful and non-deliberate systems. The deliberate system incorporates passwords, shrewd cards for signs-in data, it depends on the reaction of the client. For non-intentional procedure beat, circulatory strain and pulse are incorporated. This discovery depends on the client consequently reacting to jolt. In any case, these procedures have a few impediments of inadequacy for giving genuine outcome which causes increment preparing time, cost, and the absence of demonstrated of the right outcome. There are no reasonable criteria for sensors to identify the properties of the human body as a unique finger impression of sweat. It can't give data identified with additional properties for considering particular or common properties related to the individual in an evolving climate. So, it just distinguishes the manufactured unique mark of an individual.

2. Methodology

Using image quality assessment, we assume that the utilised image quality used for spoofing attacks has different qualities as compared to the real image. The difference includes colour, the sharpness of that image. The primary issue here is to discover the set of functions was using to categorize a picture as fake or real . It is shown in figure 1.

The major issue of fake biometric identification could be viewed as a two-class classification issue where an input sample should be allocated to one of two classes: real or fake. A novel parameterisation was proposed in this work using "25 general image quality measures". A general diagram of the suggested protection method will be illustrated in fig. 3.1. Since the approach works on the whole image without trying to find any attribute-specific properties, no pre-processing steps such as segmentation of fingerprints, iris identification or face reclamation are needed. These features restrict its computation complexity. When the feature vector was already extracted, the sample is classified into two major types: "real, generated by a genuine attribute, or fake, produced synthetically, using some essential classifiers". The parameterisation suggested in this procedure includes 25 reference and blind image quality measures. The selection process for the initial characteristics to assess the set of 25 IQMs was completed under five basic measures. The 4 criteria of selection are:

- **Performance:** Only commonly utilized methods of quality related to the image that already were accurately assessed proposing superb implementation for various applications that were viewed.
- **Complementarity:** for the purpose of generating a as general framework as possible for the attacks that have been identified and supporting biometric modalities, main concern was given to IQMs based on additional image properties such as sharpness, entropy or structure.
- **Complexity:** To maintain this method as simple as possible, features of low complexity were chosen over those that includes a higher computational burden.
- **Speed:** So as to guarantee an easy-to-use non-nosy application, clients ought not to take long for a distinguishing proof framework reaction. Subsequently the element extraction time has been given the most elevated need, which has an extremely noteworthy effect on the all-out speed of the face acknowledgement calculation.

A) Full-Reference IQ Measures (FR)

The IQA strategies rely on the availability of a clean undistorted reference image to appraise the quality of the test sample. In the challenge of fake detection discussed in this work, such a reference image is unidentified, since the discovery framework just has passage to the information test the information picture I (gray-scale, size N / M) is separated with a low-pass Gaussian piece ($\pi = 0.5$, size $3/3$) to make a smooth variant of I . At this stage, the quality between the two pictures, I and I , is determined utilizing the full reference IQA metric.

This methodology recognizes that the loss of quality caused by Gaussian scanning varies between the actual biometric features and the fake stuff. Data from studies assert the assumption.

1) Error Sensitivity Measures

Identifying the approach for reviewing image quality relies on assessing the errors for both distorted and reference images, and helping to coordinate these errors in a manner that simulates the sensitivity of human visual error. Even though their usefulness as signal fidelity evaluations is up to date to some extent debatable, these are without suspect the most commonly used methods for IQA since they properly utilize several more known psychophysical aspects of visual system of the human, they are simple to be measured and, as a rule, their computational complexity is extremely low. A

few of those parameters were included in this work's proposed 25-function parameterization. These characteristics were classified into five special categories, as demonstrated by the image property measured.

These characteristics measure the deviation between two images depending on their differences in pixel-wise direction. This work includes "Mean Squared Error (MSE), Signal to Noise Ratio (SNR), Peak Noise Ratio (PSNR), Structural Content (SC), Maximum Difference (MD), Standardized Absolute Error (NAE) and Average Difference" (AD).

- Correlation-based measures: In contexts of correlation function the between two digital photos similarity can be analyzed. Given the angle of statistical data between the pixel vectors of the original and distorted images, a variance in correlation-based measurements can be obtained. These characteristics include Mean Angle Similarity (MAS), Normalized Cross-Correlation (NCC), and Mean Angle- Similarity of Magnitude (MAMS).
- Edge-based measures: For instance, edges and other two-dimensional highlights are likely the most enlightening pieces of a picture, which has a basic job in the human visual system and numerous PC vision algorithms along with quality assessment applications. Since an image's structural distortion is intimately associated to its angle degradation, two edge-related quality measurements were considered here: Total Corner Difference (TCD) and Total Edge Difference (TED)
- Spectral distance measures: Another standard image processing tool implemented to the field of image quality assessment is the Fourier transform. In this research IQ "spectral-related features: Spectral Magnitude Error (SME) and Spectral Phase Error (SPE), where F and F are the respective Fourier I and I transforms, and $\arg(F)$ is phase-related".
- "Gradient-based measures": Gradients contain significant visual data that could be useful for the evaluation quality. An enormous proportion of distortions that is can impacting an image are shown in its gradient by adjustment. Consequently, the use of such information can adequately assess structural and contrast alterations. The biometric protection system employs two basic gradient-based features, Gradient Magnitude Error (GME) and Gradient Phase Error (GPE).

2) Structural Similarity Measures

The prior image quality metrics depending on sensitivity to errors display a few issues, their lack of matching through "subjective human-based quality scoring systems" sometimes proves this. Through this work, a new sampling frame was proposed for image quality assessment based on structural similarity, on the presumption that the human visual system is highly modified to collect structural data from the environment of viewing. Consequently, an image distortion originating from changes in lighting, such as non-structural distortions such as changes in contrast or brightness, must be considered in a different way from structural ones. The "Structural Similarity Index Measure" (SSIM) has the most straightforward implementation among this ongoing goal perceptual measures and has increased across the board prevalence in a wide scope of useful applications. The SSIM has been included in the 25-function parameterisation given its very attractive properties.

3) Information-Theoretic Measures

Through an information theory point of view, review of the information is viewed as reliability issue, instead of signal reliability. The basic thought behind these strategies is that a source of images connects with a receiver via a channel that restricts the amount of data that may travel through it, thus it introduces distortions. The objective is to incorporate the visual quality of the test image into the amount of information given between the test and the reference signals, that is, the common information between the test signals. Two of those information-theoretical features were considered in this work:

"The Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED)". The two parameters are dependent on IQA's information-theoretical perspective, nevertheless each necessitates a local or global method to the actual problem. The VIF metric predicts the quality fidelity as the ratio in between total entropy information calculated from the the whole distorted image optimally derived by the brain and the total information contained in the full reference image. Otherwise, the RRED metric approaches the QA problem from the point of view of calculating the quantity of limited information difference between the reference image and the estimation of the distorted image into the normal image space, for a provided wavelet domain sub-band. Basically, the RRED calculation quantifies the normal distinction in dispersed style between scaled local entropies of wavelet reference coefficients and projected distorted images in distributed fashion. All through this in opposition to the VIF highlight, it isn't adequate for the RRED to have passage to the entire reference picture yet just to a little piece of its data.

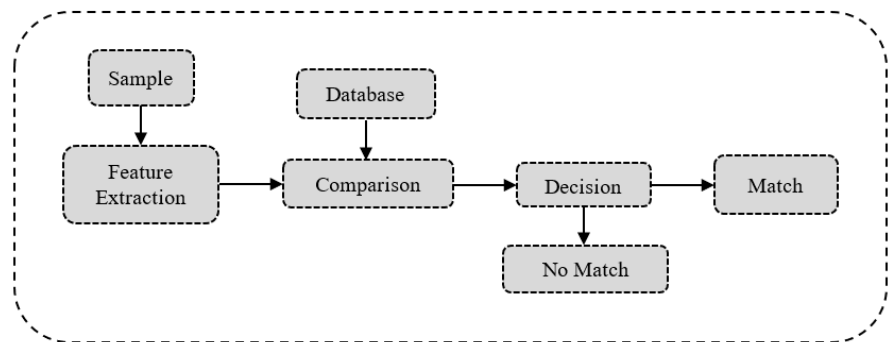


Fig. 1. General block diagram of the proposed biometric system

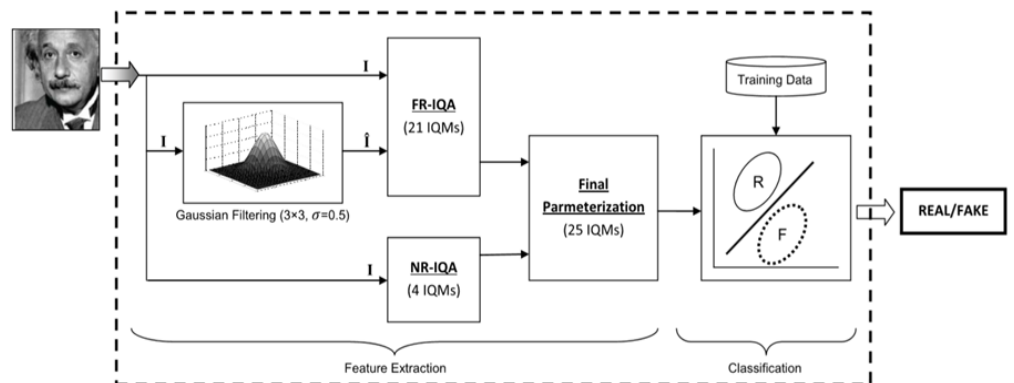


Fig. 2. General block diagram of the biometric protection scheme based on Image Quality Assessment (IQA).

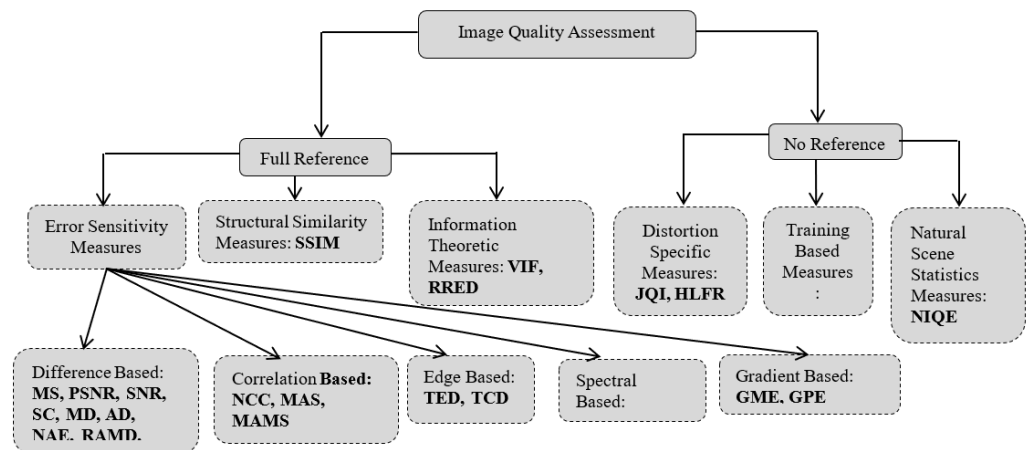


Fig. 3. Implemented 25 image quality measures classification in this work.

Only when all the "scaled entropy terms in the chosen wavelet sub-band are considered in one block, this important information may even be diminished in one scalar".

B) No-Reference IQ Measures

overall, visual arrangement of the human requires no reference test to determine the quality degree of a picture rather than the target reference IQA methods continuing to follow this equivalent hypothesis, in the absence of a reference, "automatic no-reference image quality assessment NR-IQA algorithms" attempt to address any challenging and difficult issue of image quality assessment. At present, "NR-IQA methods estimate the quality of the test image by some pre-trained mathematical analyzes".

- **Distortion-specific approaches:** These strategies rely on background data of the sort of loss in visual quality that a particular distortion caused it. The final quality measurement is calculated using a model that have been taught by clean image usage and images which are influenced by this special distortion. 2 of measures were connected to the biometric strategy for security suggested in this piece of work. The "JPEG Quality Index" (JQI), which assess the quality of images strongly impacted by common block artifacts found in many low-bit compression algorithms, such as the JPEG. The High-Low Frequency Index (HLFI) is highly affected by past work that looked at regional gradients as a blind metric for the noise and blur identification. Similarly, the HLFI function is sensitive to image sharpness by calculating the difference between lower and upper frequencies of the Fourier Spectrum power.
- **Training-based approaches:** Based on the prior NR-IQA methods class, a system is built using clean and distorted images in this kind of techniques. The quality score is then calculated on the basis of several functions has been derived of the test image and has been linked to the typical model. However, these metrics, in contrast to the earlier methods have a tendency to give a particular score of quality has no relation to a particular distortion. The statistical model was qualified to this final stages with images that are influenced by various types of distortion. This is the circumstance with the Blind Image Quality Index (BIQI) some portion of the 25 list of capabilities appeared in this study. The BIQI follows a two-phase structure in which the different bending explicit specialists' individual measures are joined to create one worldwide quality score.
- **Statistical approaches to natural scene:** All such blind IQA methods utilize information obtained from distortion-free natural scene of images to educate the initial model. The reasoning of this trend is different depending on the theory that undistorted natural environment images present specific frequent properties of all probable images that fall within that subspace. Differences from the natural statistics consistency can, if accurately evaluated, assess the conceptual image quality. This procedure is adopted by The "Natural Image Quality Evaluator" (NIQE) utilized in the current investigation follows this research. The NIQE is a totally blind image quality analyzer depending on the development of a quality-aware collection of statistical features linked to a statistical model of the multi-variety Gaussian natural scene. Result Analysis and Discussion

1) Quality Parameters

During conducting the watermarking scheme on the cover image, various quality parameters such as Peak Signal to Noise Ratio (PSNR), Correlation Factor, and Total Time Elapsed in Second have been taken into account.

Peak-Signal to Noise Ratio (PSNR): Differences from the natural statistics consistency can, if accurately evaluated, assess the perceptual feature of a picture. This procedure is adopted via "The Natural Image Quality Evaluator (NIQE)" utilized in the

current investigation follows this research, in certain circumstances, thusly, one reconstruction may appear to be closer to the past model form than another, and regardless of whether it has a lower PSNR (a higher PSNR would typically recommend that the recreation is of more prominent quality). It is depicted by for the most part methods for MSE (mean square error). PSNR is shown in the logarithmic decibel scale.

The PSNR (in dB) is defined as:

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{\text{MAX}_I^2}{\text{MSE}} \right) \quad (1)$$

$$\text{Where, } \text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Where MAX_I is the maximum possible pixel value of image I(i,j). MSE is a mean square error. I(i,j) is an original cover image. K(i,j) is a reconstructed cover image. m is the number of rows and n is the number of columns.

Mean Squared Error (MSE): "The mean squared error MSE of a measure is the squares average of the errors, that the variation between both the estimator and estimated value". The equation is given by,

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (2)$$

Structural Content (SC): "It is defined as the ratio between the square of the sum of the original image and reference image". The equation is given by,

$$\text{SC}(I, K) = \frac{\sum_{i=1}^N \sum_{j=1}^M (I(i,j))^2}{\sum_{i=1}^N \sum_{j=1}^M (K(i,j))^2} \quad (3)$$

Average Difference (AD): Absolute difference image average value is estimated for every pixel (original image is detracted to the reference image). The equation is given by,

$$\text{AD}(I, K) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M |I(i,j) - K(i,j)| \quad (4)$$

Normalized Absolute Error (NAE): It is defined "as the ratio between the sum of absolute difference image and absolute of the original image". The equation is given by,

$$\text{NAE}(I, K) = \frac{\sum_{i=1}^N \sum_{j=1}^M |I(i,j) - K(i,j)|}{\sum_{i=1}^N \sum_{j=1}^M |I(i,j)|} \quad (5)$$

Signal to Noise Ratio (SNR): Signal-to - noise ratio (demonstrated as SNR or S / N) is a way of measuring used in business and science that differs the required level of signal with that of background noise. It is the signal-to - noise ratio, expressed in the decibels, a ratio higher than 1:1 (significantly higher than 0 dB) indicates a signal greater than a noise. An electrical signal is a form of a signal applied to an SNR. The Shannon – Hartley theorem connects the SNR, a channel communication capability, and the channel bandwidth. The signal-to - noise ratio is seldom used in a discussion or exchange to refer to the ratio of useful information to false or unrelated data. In online discussion councils as well as other online communities, for example, junk is considered a "noise" that prevents the "signal" of correct

$$\text{conversation. } \text{SNR}(I, K) = 10 \log \left(\frac{\sum_{i=1}^N \sum_{j=1}^M (I(i,j))^2}{N \cdot M \cdot \text{MSE}(I, K)} \right) \quad (6)$$

Maximum Difference (MD): The maximum value of the absolute difference image (the original image is detracted from the reference image) is approximated. The equation is provided by,

$$\text{MD}(I, K) = \max [I_{i,j} - K_{i,j}] \quad (7)$$

Blind Image Quality Index Measurement (BIQI): Blind IQA strategies have been using a previous data obtained from alteration-free natural scene pictures to prepare the original model. The aim was behind this propensity depends on the hypothesis that unmistakable world pictures normally present certain standard attributes that fall inside

a safe subspace of every single imaginable image. Deviations from the consistency of regular review information can appraise the perceptual nature of a picture if appropriately registered.

2) Result for Iris

We can compare iris parameters of the input image with database information.

For first sample:

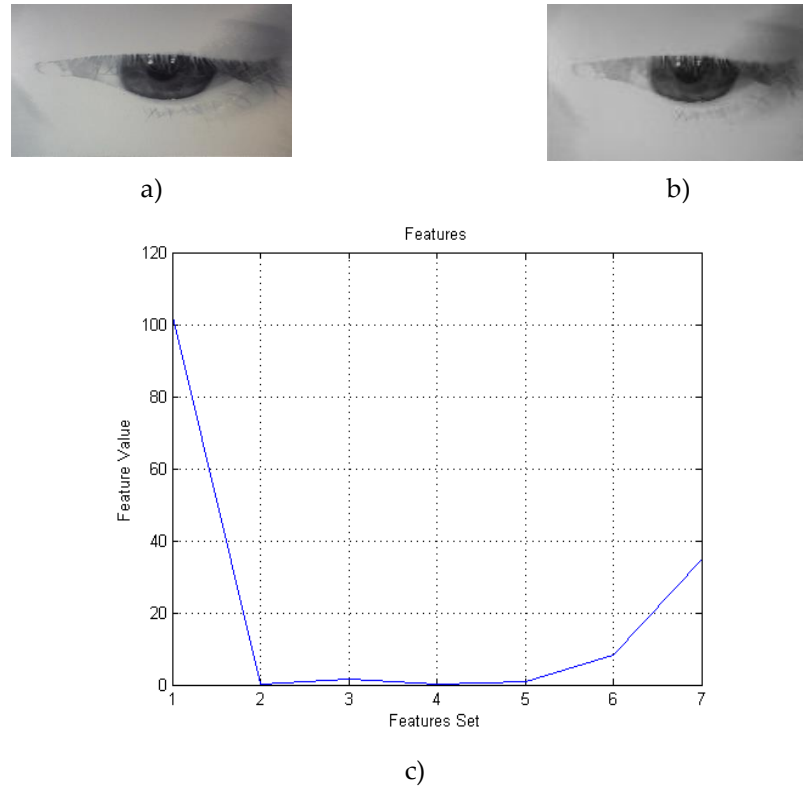


Fig. 4. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

Table 1. Calculations of values for different parameters

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	102.985
2	Mean Square Error (MSE)	1.4996
3	Structural Content (SC)	1.00104
4	Average Difference (AD)	0.0799574
5	Normalized Absolute Error (NAE)	0.0005414
6	Signal to noise ratio (SNR)	8.10403
7	Maximum Difference (MD)	35
8	Training Based Measure (BIQI)	3.03668e-05

The result obtained for the above image is: It's a Fake Biometric

For Second sample:



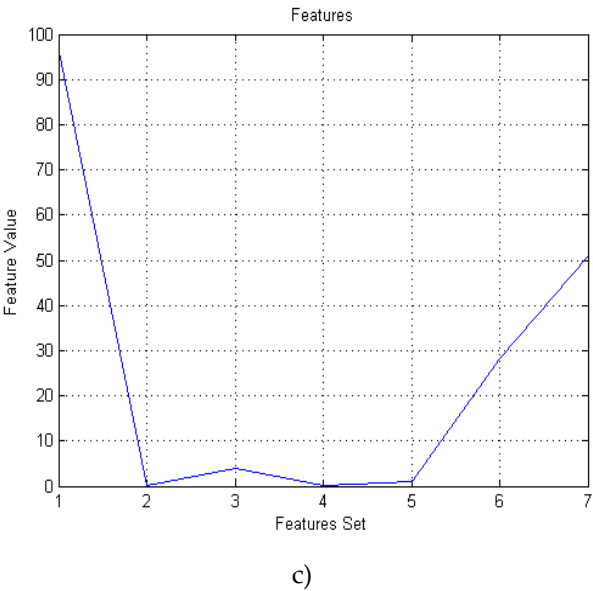


Fig. 5. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

Table 2. Calculations of values for different parameters		
Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	96.7474
2	Mean Square Error (MSE)	4.0869
3	Structural Content (SC)	1.00137
4	Average Difference (AD)	0.150274
5	Normalized Absolute Error (NAE)	0.0006768
6	Signal to noise ratio (SNR)	28.1557
7	Maximum Difference (MD)	51
8	Training Based Measure (BIQI)	8.2524e-05

The result obtained for the above image is: It's a Real Biometric

3) Result for Fingerprint

We can compare the thumb parameters of the input image with database information.

For Second sample:



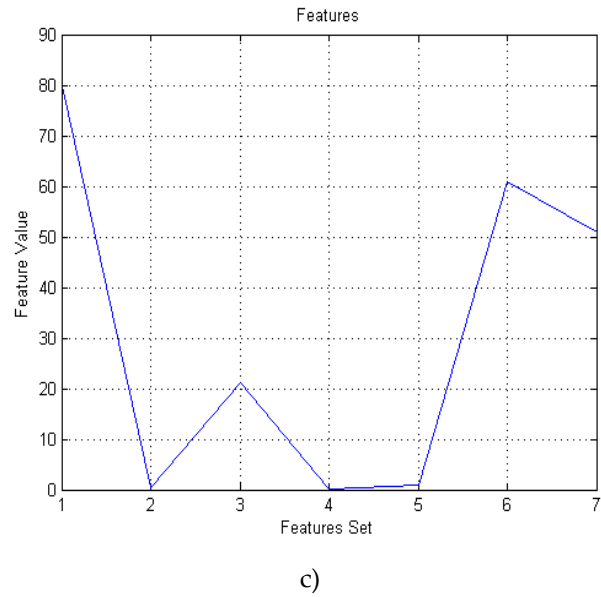


Fig. 6. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

Table 3. Calculations of values for different parameters

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	80.3138
2	Mean Square Error (MSE)	21.1395
3	Structural Content (SC)	1.00768
4	Average Difference (AD)	0.278144
5	Normalized Absolute Error (NAE)	0.0012610
6	Signal to noise ratio (SNR)	61.0228
7	Maximum Difference (MD)	51
8	Training Based Measure (BIQI)	0.0276939

The result obtained for the above image is: It's a Real Biometric

For Second sample:



a)



b)

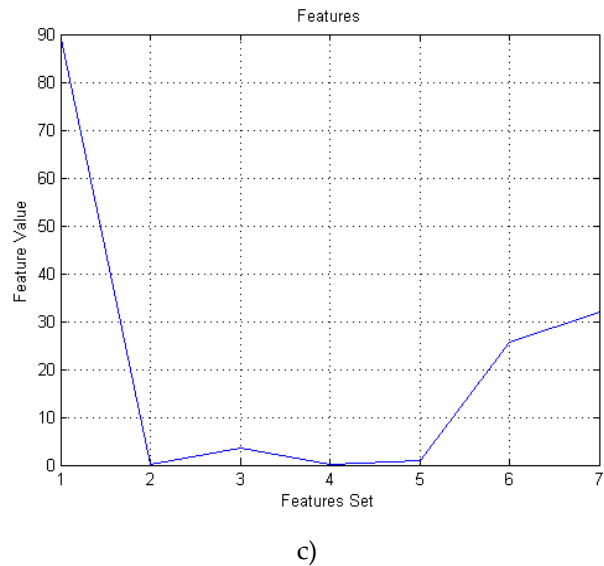


Fig. 7. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

Table 4. Calculations of values for different parameters

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	89.6621
2	Mean Square Error (MSE)	3.60282
3	Structural Content (SC)	1.00303
4	Average Difference (AD)	0.175285
5	Normalized Absolute Error (NAE)	0.0012111
6	Signal to noise ratio (SNR)	25.6343
7	Maximum Difference (MD)	32
8	Training Based Measure (BIQI)	3.10663e-005

4) Result for Face recognition

We can compare the face parameters of the input image with database information
For first sample:



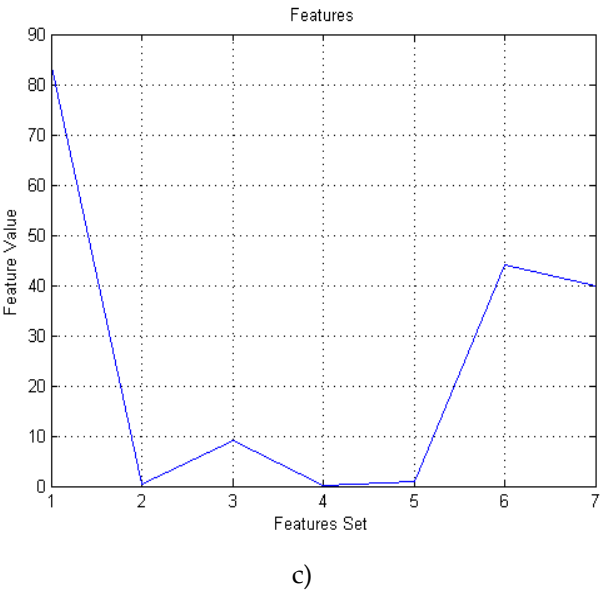


Fig. 8. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

Table 5. Calculations of values for different parameters

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	83.1288
2	Mean Square Error (MSE)	9.025
3	Structural Content (SC)	1.0002
4	Average Difference (AD)	0.4005
5	Normalized Absolute Error (NAE)	0.00267
6	Signal to noise ratio (SNR)	43.1506
7	Maximum Difference (MD)	40.02
8	Training Based Measure (BIQI)	4.01243e-005

The result obtained for the above image is: It's a Fake Biometric

For Second sample:



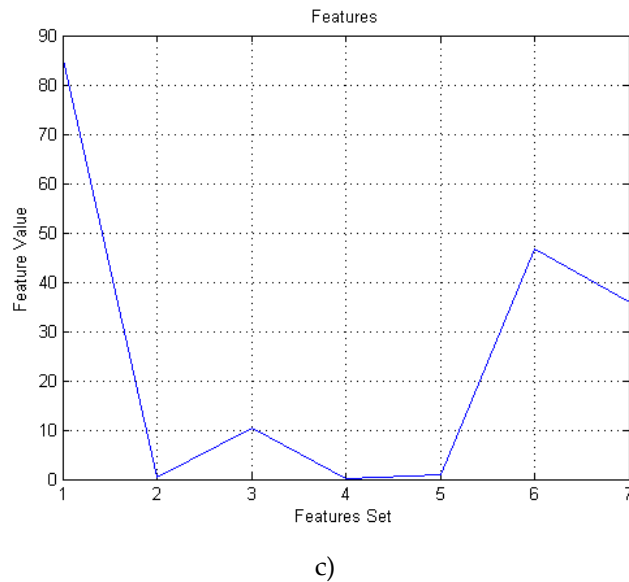


Fig. 9. Result analysis of the figure of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters

Table 6. Calculations of values for different parameters

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	84.6073
2	Mean Square Error (MSE)	10.30052
3	Structural Content (SC)	1.00072
4	Average Difference (AD)	0.32058
5	Normalized Absolute Error (NAE)	0.00550385
6	Signal to noise ratio (SNR)	45.5269
7	Maximum Difference (MD)	36.02
8	Training Based Measure (BIQI)	0.0031456

The result obtained for the above image is: It's a Real Biometric

3. Conclusion

The current development of the Biometric framework expanded so there is a requirement for insurance of that framework. Picture quality evaluation is the method utilized for recognizing genuine and counterfeit picture. It likewise gives multi-biometric and multi assault assurance highlight to the framework because of this the security level is expanded. By looking at all highlights or parameters of the example it gives the proficient outcome. With the assistance of novel programming and picture quality appraisal, it gives a quick reaction. For this reason, we will consider 8 general picture quality parameters. The novel technique executed for various biometric modalities like iris, fingerprint, and face utilizing publicly accessible database data. The biometric recognizable proof framework gives a precise outcome with simple and safe utilize. Likewise, programming and equipment are easy to use without the need for an additional piece of establishment and treatment of framework. it finishes its activity inside a few seconds, so it is efficient. This framework is utilized for office or different applications like login reason. Since the utilization of biometric property of the human body, it can't be stolen or speculated by someone else, consequently, it is having long execution for the utilization in the organization. Rather than utilizing the digit secret word, we can utilize the physical highlights of the human body. The biometric framework considers as advantageous security arrangement since client can't require any ID confirmation, watchword which is hard to deal with consistently for login framework.

REFERENCES

- [1] Javier. Galbally, Sebastien Marcel, Member, IEEE, and Julia Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition.", *IEEE Transactions On Image Processing*, Vol.23, No.2, February 2014.
- [2] Javier. Galbally, Chris McCool, Julian Fierrez, Sebastien Marcel, and Javier Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," *Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.
- [3] Sarvesh Manav Meena, Prof. Arun B. Nandurbarkar "A Literature review on liveness assessment of Multimodal Biometrics through Image Quality Assessment" *IJSTE*.Vol.2,Issue-08,February 2016.
- [4] Yujia Jiang & Xin Liu "Spoof fingerprint detection based on co-occurrence matrix" *International journal of signal processing, image processing and pattern recognition* Vol 8, No. 8, pp. 373-384, 2015.
- [5] S Chinthu, C. Dhanabal "Fake identification in fingerprint, Iris and face recognition using Image Quality Assessment", *IJARSE* Vol. no. 4, Issue no. 02, February 2015.
- [6] Tija Thomas, Helice K Babu, Ambikadevi Amma T. "A novel fake detection system for biometric modalities", *IJARCSSE*, Volume 5, Issue no. 4, 2015.
- [7] M. S. Aleena T. A., Ms. Chithra. K., Mr. Rahul Ramachdran" Spoofing protection for biometric system", *IJSTE*, volume 1, Issue 10, April 2015.
- [8] Anju. M. I., G. Sheeba, G. Sivakami, Monika. J., Savitri. M., "Multimodal biometric recognition security system", *IJAREETE*, volume.4, Issue 3, March 2015.
- [9] Maria G. Martini, Chaminda T.E.R. Hewage, Barbara Villarini, "Image quality assessment based on edge preservation," *Signal Process., Image Commun.*, vol. 27, no. 8, pp. 875–882, 2012.
- [9] Mojtaba Sepasian, Cristnel Mares, Wamadewa Balchandran, "Liveness and spoofing in fingerprint identification: Issues and Challenges" *Recent advances in Computer Engineering & Applications*, pp. 150-158.
- [10] Arjun Nichal et. al "Face Recognition using PCA and Eigen Face," *International Journal of Innovative Research in Electrical, Electronics, Instrumentation & Control Engineering*, Vol. 2, Issue 5, pp. 1435-1438, May 2014.
- [11] Arjun Nichal et. al "DCT Based Iris Feature Extraction and Recognition for Security System" *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 5, pp. 6490-6494, May 2014.
- [12] Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2010). Fingerprint liveness detection based on quality measures. *Pattern Recognition*, 43(1), 271-283. <https://doi.org/10.1016/j.patcog.2009.06.014>
- [13] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2, 1530-1552. <https://doi.org/10.1109/ACCESS.2014.2381273>
- [14] Galbally, J., McCool, C., & Marcel, S. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, 23(2), 710-724. <https://doi.org/10.1109/TIP.2013.2293423>
- [15] Meena, S. M., & Nandurbarkar, A. B. (2016). Liveness evaluation at multimodal biometrics through the picture quality appraisal. *International Journal of Computer Applications*, 135(6), 21-26. <https://doi.org/10.5120/ijca2016908765>
- [16] Thomas, T., Babu, H. K., & Amma, A. T. (2015). A novel fake detection system for biometric modalities using image quality assessment. *Journal of Computer Science*, 11(5), 674-683. <https://doi.org/10.3844/jcssp.2015.674.683>
- [17] Sepasian, M., Soryani, M., & Fathy, M. (2010). A novel fingerprint liveness detection technique using quality-related features. *Forensic Science International*, 207(1-3), 1-9. <https://doi.org/10.1016/j.forsciint.2010.01.018>