International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

Enhancing Biometric Security: A Framework for Detecting and Preventing False Identification

Hayat Al-Dmour
Faculty of Information Technology
Mutah University
Karak, Jordan
Hdmour@mutah.edu.jo

Abstract— Biometrics is a technological system that utilizes data to differentiate one individual from another. The biometric framework can be used by government and private organizations for security purposes. This software-based technology helps to look at an individual's data if it is genuine or fake. The study suggested a framework; its goal is to strengthen the development and acceptance of the biometric system. The function of this system is to reduce the applied effort to identify and recognize the quality of the image in less time. This study utilizes three data applications: iris, fingerprint, and face recognition. The approach proposed by the survey uses different features of the images to determine the difference between the original image and the considered sample image. It gives efficient protection against different spoofing attacks. Simulation results show that the high-quality detection application has an average peak signal-to-noise ratio (PNSR) of 89.77. Further, the proposed model effectively detects false biometric identification.

Keywords- fake biometric detection; image quality; face and fingerprint; protection; spoofing; iris; biometrics.

I. INTRODUCTION

The fourth industrial revolution (4IR) has brought rapid change in all areas of life. Advances in technology have forced individuals and societies to adapt to changes by developing skill sets or perish [1]. New technologies include wireless tools, the internet, artificial intelligence, 3D printing, cloud computing, and robotics. So, technologies are evolving, and so is the security related to it. ”Fingerprints cannot lie, but liars can make fingerprints” is an old quote which is most popular among researchers. The quote says needs to be modified because now the intruders and spoof makers are making spoofs of every biometric, which is available for use in the present technology [2]. With the rapid advancement in technology comes the threat of cyber security and invasion of privacy.

Biometric recognition represents a spontaneous acknowledgment of individuals computationally. According to the study, [3] to observe and investigate the anatomical features and patterns of individuals, the system of biometrics is one of the recommendations. The main advantage of biometric authentication could also be seen as a disadvantage. Biometrics allows us to uniquely identify one person, but this also raises the question of privacy issues [4]. Sharing your biometric traits such as fingerprints or face scans may feel 8 more intrusive than just picking a password for authentication. Biometric data contains a lot more information about a person than a password or PIN code. To overcome problems such as spoof attacks, poor input data quality, non-universality, etc. multimodal biometric systems came into existence [5]. A biometric recognition system consists of two phases. The first is the enrolment phase in which the biometric data is registered in the biometric system’s database. The second is the authentication phase in which an individual’s recently acquired biometric data is compared to the enrolled biometric data [6]. Sensors, feature extraction, and matching modules are included in this system [7]. Moreover, this approach introduces a multi-biometric system. The biometric system can be protected from fake attacks using Image Quality Assessment.

The physiological characteristics of the human being are entirely dependent on the size of its body part. For example, facial features, shape, size of the fingerprint, etc. Fingerprint recognition is the most popular biometric technology currently used as an identifier due to the practicality and low price of the procedure. Every person has a different fingerprint, so it is considered unique. Twins even have different fingerprints [8],[6]. In the field of sense detection, to improve the security check, some specific body parts are used for scanning details to feed into the detection application. For example: In every organization, the left-hand and right-hand thumb or the fingerprint are required because of the special pattern of the finger ridges, the upper layer of the skin, and the topmost part of the finger is very important for scanning purposes. Hence, fingerprinting is one of the common methods to be used in biometric identification.

In some cases, hand sensations are not able to be detected by the detectors easily, or in sensitive cases, the Eye iris can also be used in the identification of biometric information. There are differences in the individuality of segments on the hands of every human being, similarly, there are different colors, complex networks of neuronal arrangement, and sizes in Iris. Every iris has its unique identification and always different identification from one another. Similarly in the human body, the human face has a unique property, and it can be recognized easily by the face recognition system. According to the study [9], face recognition is one of the specific systems that identifies the face from the swarm easily. This system has a special identification database that collects information based on features like the measurement of landmarks, nodes, valleys, and peaks. This system identifies the features only while it does not work on behavioral characteristics that are associated with the signature, voice of the individual, etc.

The Biometrics system works on three principles: (1) Sensation of the object (2) Unsheathing feature of the object (3)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

Recognizing and matching link of the module [2]. The classification of the Biometrics system is comprised of two groups: (a) based on Hardware Technique and (b) based on Software technique. In hardware-based techniques, sensors are used to detect the senses of the selected body parts of the human subject. For example, heartbeat count, skin pattern of fingers (prints of finger or thumb), size, shape, and properties of reflection of Iris in the eye, and perspiration if individual. There are selective sensing devices that are used to measure the parameters of the Iris, hand prints, and study palmistry. In software-based techniques, helps to generate the comparison between fake and original features [10]. These two types of methods have some advantages and drawbacks. Therefore, a biometric system provides a complete and strong security system through the coherence of both methods. The function of the hardware scheme is to detect every level of counterfeit sensation as a coarse comparison and vice versa, in the function of the software technique no other detection element is required, very economical and crystal transparent to the end user. It also consists of facial trait recognition and directly obtains from the obtained feature. This also allows for the identification of additional illegal break-in attempts that are not always characterized as spoofing assaults [11].

The biometric system can be protected from fake attacks using Image Quality Assessment. The image of the organs can be differentiated by size, shape, color, etc., for example, the appearance of the face, general features of the iris, the pattern of fingerprint, etc. Iris scanning and fingerprint recognition are the most familiar techniques of biometric security [12]. According to the study, to identify the quality of an image, a technique is used known as Image Quality Assessment (IQA). This technique works on mathematical equations to analyze the originality of a biometric identifier. Digital images are prone to spoofing and aberrations during any stage of image processing [13]. Image irregularities can occur at the compression, storage, processing, reproduction, and transmission stages of image processing. Objective and subjective visual quality assessments are the two kinds of image quality assessments.

The objective quality assessment method is categorized based on a reference image that is of perfect quality and is free of distortion. In the assessment, there are three classifications to understand the objectives of the assessment. (i) Image quality assessment based on Full-reference (FR-IQA), (ii) Image quality assessment based on reduced-reference (RR-IQA), and (iii) Image quality assessment based on no-reference (NR-IQA). The subjective quality assessment method is considered to be the most dependable method to analyze image quality. In this quality assessment, the views of a group of people are collected concerning the quality of each image. However, the flaws of subjective testing are that it is impractical and expensive.

There has been substantial progress in the development of biometric recognition structures for the detection of direct attacks in biometrics [2]. On the other hand, spoofing mechanisms have also grown exponentially. Subsequently, effective and new protection measures are being explored and developed. The present study offers an innovative software-based multi-attack and multi-biometric security technique by using the methods of image quality assessment. The novelty of this study lies in the development of a software based multi-attack and multi-biometric security technique that uses image quality assessment methods. The technique is designed to detect direct attacks and spoofing mechanisms with low complexity and high-speed features, enabling real-time functioning. The study utilizes general image quality measures and simple classifiers that are fast to compute, without relying on features such as face detection minutiae points or iris position. This approach is unique and innovative in the field of biometric recognition, as it offers a new and effective protection measure against attacks on biometric systems.

The rest of the paper is organized as follows: Section 2 presents the Literature review that has the past studies. The methodology is presented in Section 3. Section 4 is a similarity measures section where similar measurement models are presented, and Section 5 presents approaches to be taken. Section 6 presents analysis and discussion, and the last section 7 presents the conclusions drawn from the study.

II. Literature Review

In [11], an overview of the process of image quality measurement for liveness assessment of biometric modalities was introduced. In that image quality, parameters are utilized to separate genuine and fake pictures. The image quality appraisal has two sections; the first part is subjective. Information is contrasted, and the positioning of parameters after that outcome is shown in five classes; extremely poor, poor, grand, and magnificent. Subsequently, this technique offers positioning to test if the most extreme element matches a unique example. It gives a brilliant rank, or if there are fewer matches amongst information and unique examples, it provides an inferior rank to the framework. The second part is the objective, which comprises two images; one is for reference, and another is a test picture.

Galbally et al. proposed image quality-related parameters for iris recognition. Iris can be distinguished by a few properties like concentration and impediment which identify the structure of eyelashes [2]. Zhou et al. proposed a new all-inclusive image quality list which is anything but challenging to materialize different pictures when preparing an application. It comprises parameters like loss of connection. It measures the linear relationship between X and Y and luminance blending [14].

Galbally et al. conducted Sebastian Marcel research covering all the aspects that are related to the methodologies and applications used in the identification of detection. The recognition methods were applied to 25 picture characteristics by multiple resources. Those characteristics are contrasting and counterfeit testing pictures. This paper employed a general picture quality parameter to recognize genuine and fake examples. It uses MATLAB programming. This framework has multitasked and multi-biometric insurance techniques [10].

Jiang and Liu proposed fake unique finger impression identification. In this study, co-event frameworks or novel programming utilize most parts. It comprises a counterfeit distinctive mark made using materials like gelatin or silicon. It has diverse strategies like sweat pore-based, skin flexibility, surface, etc. Likewise, it has highlighted the extraction process, in which one of the strategies is called the preparing strategy, which is used to make a judgment, and the other is the trying procedure, which is meant to look at the picture. It includes extraction, and the picture pixel is quantized. Quantization will cause data loss, which is the weakness of this task [15].

In 2015, Chinthu and Dhanabal proposed a counterfeit to distinguish finger, iris, and face proof by utilizing picture quality appraisal. In this novel, programming is used to catch unique

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

pictures to improve quality. Catch pictures are imprinted on paper utilizing a business printer and accessible at the sensor. Framework engineering comprises diverse modules for a location like aliveness recognition and assault on the biometric distinguishing proof framework. The framework handles distinctive assaults and gives abnormal state assurance by using this. The assault on a framework like unique pictures is for better quality, imprinted on the business printer's clips. Utilizing this data or printed images displayed on a sensor of the biometric framework. This framework is caught and contrasted by programming and identifies that information is genuine to the framework. This framework uses distinctive techniques like histogram leveling and diminishing pictures (it is the change of an advanced picture into a streamlined one). By breaking down this parameter, a discovery result is made. It gives an abnormal state of security over various sorts of assaults. For examining parameters, it needs high-caliber pictures [16].

Ramachandran proposed a security enhancement for a biometric framework that used Gaussian separation combined with Fourier transformation. The proposed framework demonstrated its capability to undertake a multilevel task when assessing a device, resulting in a 90% accuracy rate. By utilizing extracted image quality measures, it distinguishes between genuine and counterfeit input images. This system comprised a complete reference utilizing database information for analysis. It ensured that no reference database data was missing, employing various methodologies including distortion-specific techniques such as JPEG quality files and High-Low frequency files, along with a training-based approach that processes both clean and distorted images. Additionally, it employed a typical scene static approach to gather information related to the Gaussian filter [17].

Martini et al. introduced an approach for assessing image quality, specifically focusing on edge preservation. Their study proposed a transmission edge discovery technique, aimed at addressing the subjective nature inherent in evaluating images, which holds significance in both the design and assessment of image compression methods. The precise identification of critical image elements to be transmitted remains a crucial aspect. Within transmission systems, evaluating image quality metrics at the receiving end provides valuable feedback to system controllers, enabling the establishment of target quality metrics without unnecessary reliance on references for original images. Human visual perception is known for its sensitivity, and the information embedded in image layouts supports the proposal of a reduced-reference quality metric. This approach helps mitigate the drawbacks associated with low boundary estimations that lead to heightened sensitivity around edges. When boundary measures are excessively high, it results in significant portions of the image being categorized as edges, which can be inconsequential for accurate quality assessment [17].

Sepasian et al. (2009) introduced a method for identifying spoofing attacks associated with fingerprints. The proposed approach aimed to differentiate between genuine and fake fingerprint images. Additional software procedures were employed to detect spoofing attacks. The methodology involved various authentication measures such as passwords, smart cards, and user responses, relying on the user's reaction. In addition to intentional measures, non-intentional processes such as monitoring pulse, blood pressure, and heartbeat were integrated. However, these methods have exhibited limitations, including their inefficacy in providing accurate results, leading to increased time and cost, alongside a lack of substantiated outcomes [18].

Fu et al. investigated facial features, encompassing eyes, mouth, and nose, alongside their utilitarian aspects within the context of general image quality assessment (IQA) metrics. Their study aimed to uncover the relative significance of these facial components. However, the research primarily centered on IQA metrics, thereby limiting its contribution to understanding the explain ability of Facial Image Quality Assessment (FIQA) [19]. Subsequent studies have delved deeper, examining the impact of various sample categories, such as low and high quality, on these features. Additionally, they have explored spatial activation maps derived from supervised FIQA and IQA methods, as well as their application to masked faces [20].

III. METHODOLOGY

A. Principle

The principle of biometric authentication is that each individual can be correctly identified by fundamental physical or behavioral traits. The classification of the sample selected for the biometric will be having an original identity or fake identity. A suitable classifier examines the authenticity of the image by extracting a set of distinct features. In this study, three data applications are used: iris, fingerprints, and face recognition. The 25 general image quality assessment processes through a unique parameterization technique. The validation of images includes the variance based on quality. The fake and the original quality consist of image quality factors such as degree of sharpness, brightness and color contrast levels, and local artifacts. Furthermore, the quality variance may also involve natural appearance, structural distortions, and the aggregate of information found in both kinds of images. Some of the features in mobiles also have the techniques to capture images under/overexposed. The results of the fingerprint depend on the surface of the skin if it is sticky in appearance the marks of patches and spots will be available in the image also. Another illustration includes blurry iris images captured from the printed paper due to shuddering.

In a contingency where an image produced falsely can be processed in the development of a channel before the image is applied in figure form. The forged image does not have all the original elements of the image. After the hypothesis, the potential difference in the quality general image quality assessment is scrutinized in the current study as a protection method of biometric technique to work as a counter plan. The employed structures have to develop the calculation on a specific attack or a given biometric approach. This makes it easy to compute distinct features on any image. A unique multi-biometric dimension is explored in the present study. The suggested method of the study is not used in any other studies and even it is not used as a strategic scheme to protect the biometric system.

B. IQA Features Methodology

This methodology presents a unique study, three factors reinforce the justification of applying the detection methods in the upgraded version of IQA features:

- In the field of criminology, image assessment has the most versatile usage and implication for both steganalysis [21] and image manipulation detection

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

[22]. The current study shows that spoofing attacks with printed face images or iris are image manipulation attacks. Spoofing attacks can be detected successfully using diverse quality features.

- Preceding studies in the criminologist field have used diverse features to compute trait-specific quality properties for the aim of liveness detection in the iris and fingerprint applications [23].

Although steganalysis and image manipulation detection provide a good foundation for IQA as a biometric protection method, these methods are not functional both for iris and fingerprint applications. For example, to calculate the dimension and its related frequency of the evidence of spoofs of fingerprint, the image, and print of fingerprint can be used instead of the live response of the iris. Alternatively, the parameter of the bulging appearance of the eye is also considered as the anti-spoofing iris method but cannot be used to identify a fake fingerprint. Many studies provide insightful solutions to provide biometric protection, but they fail to provide a universal solution to spoofing attacks. The solutions are explicitly designed for different modalities. In subjective analysis, individual observers very frequently determine the appearance in the shape or size of the original and the fake sample and are unable to distinguish the difference. In the above-mentioned study, several techniques and computational strategies are considered for IQA to propose to achieve the perceived appearance of images by humans in a consistent manner.

The phenomena used in the assessment of the quality of the image is considered that the quality of the image completely provides helps in the spoofing attacks which have a different impact on the actual image. The difference includes the color and sharpness of the picture. Here, the main thing is to find a set of features that represent the accurate method to distinguish between the original and the fake as shown in Figure 1.

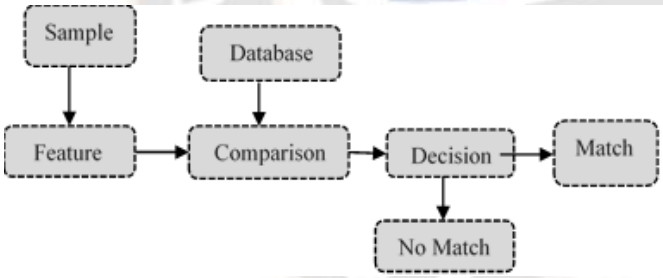

Figure 1. General Block Diagram of Biometric system.

C. Problems Reported in Biometric System

There are two problems reported in the detection of fake images in the system of Biometric. The classification consists of pain where the biometric sample is categorized into real or fake. This study proposes a strategy of selecting 25 images having measures of good quality of the image. As shown in Figure 1, there is a proposed model representing the protection approach. This method is modified based on the whole image in which no specific trait properties are selected.

There are no specific steps to start the procedure which are identification of fingerprint, iris, and face detection. This step has converted all the extra load computational software into zero. The system directly starts operating using a vector, in this, the sample is divided into many parts. The selected sample can be genuine or synthetically produced by the source using a classifier that can be fitted in the sample. The selected sample in the study includes all the references for measuring the image quality and it follows the policy of blind.

D. Specific Criteria of the System

According to the references of the literature, all the proposed methods and the perspectives approaches of IQA cannot be implemented. The process to start the first step of the study was to determine the IQMs of all the selected 25 selected samples which were categorized into 4 individual setups. After following the procedure, the last step of methodology will be applied to fulfill the requirement of the live data detection system. These four individual setups or the base of the criteria are:

- The performance or the execution: The good quality of the image, has been approved for good test consistency and the performance of the application presents that It has been observed if the good quality of the image is used in the application regularly the product will be more presentable and clear.
- Complementary: The study has supported the theory of IQMs based on the properties that are complementary to the system, (alignment of the structure, and the contrast level of sharpness). This initiative has helped the system to generate and detect the mode and the direction of the attacker in the biometric system.
- Complexity: In the processing of the system, high technology, and the heavy computational load is preferred, the selected defined method was simple, and only adequate complex feature was used.
- Speed: To improve the quality of the recognition system, make it user-friendly user access, and minimize the feature determination time, great emphasis has been given to the processing speed of the system, which significantly impacts the overall speed of the face detection algorithm.

E. Classifications of Objectives in Assessment

1) Measures on Full-reference (FR-IQA)

This method depends upon some of the factors. The factors are the requirement of a clear clean image, and the quality of the test sample will be better if the reference sample is free from all kinds of distortion. The selected reference samples are unknown, as the detection system only has access to the input sample, which may lead to the cause of fake detection. If in the system, the grey-scale image I (of size $N \times M$) is installed with filtered low-pass Gaussian kernel ($\sigma = 0.5$ and size 3×3) it will produce a smooth and clear version $\hat{I}$.

Hence, the quality of the image between the range of (I and $\hat{I}$) will produce the computer-based data following the metric pattern of full-reference IQA. This systematic method concludes with the quality loss of Gaussian filtering. This will determine the differences between real and fake biometric samples. The experimental results confirm this assumption.

2) Application of FR-IQMs

To evaluate the quality of the test sample, the method that has been used in the study depends on the availability and access of clear and accurate reference images. Since the detection

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

system in the present study only has access to the input sample, a full-reference image is unknown. This strategy has been used for practical practices of unauthentic activities, like detection in the manipulation of images and steganalysis. This is considered a limitation of the study [24], [25].

F. Measures to be taken to control Sensitivity Error

The measures are required to direct the approaches of quality of image assessment. There is a requirement to understand the errors between the selected recommended sample and the unclear sample. These steps can help to attempt, to classify the defects to simulate the human visual error sensitivity feature. The methods for IQA are based on efficiency and the measure that can be taken with fidelity signal.

There are many controversies related to the features of human psychophysical. It was defined that they can be measured on the low complexity measure of computation and the parameters can be calculated efficiently and quickly. About 25 psycho-physical features have been collected for this study and on every feature, many of the metrics have been applied. For a better understanding of the proposed method, the features have been divided into five different groups based on measurement in the image property.

1) Measures for Pixel Disparity

This element of the image is the main constituent. Based on this element, many images have clear quantification. This enables the individual to generate and develop the understanding to identify the difference between unclear, misprinted features of the two images. The methods which have implemented in this study are the calculation of Structural Content (SC), Average Difference (AD), Mean Squared Error (MSE), Signal Noise Ratio (SNR), Peak Signal Noise Ratio (PSNR), Maximum Difference (MD), and Normalized Absolute Error (NAE).

2) Measures to Correlate the Images

The function to create the similarity link between the digital images is the correlation. This is obtained by the statistical analysis of the vector in pixels and the associated angles of the fake and original image. These functional features are Mean Angle Similarity (MAS), Normalized Cross-Correlation (NXC), and Mean Angle- Magnitude Similarity (MAMS).

3) Measure to consider the Edge base of the image

The dimensions of the edges in the image has much information. This detail has great importance in the accountability of human visual systems and computer applications which deal with algorithms of visual sciences and the quality of image assessment. It has been observed that the quality of the image is based on the distortion of the structure and the closely linked with the degradation of the edge. The main quality measures of the two images are Total Corner Difference (TCD) and Total Edge Difference (TED).

4) Measures to be taken of Spectral distance in the image

Many measures can be taken on the spectral distance in the quality image assessment. The most traditional and frequently used technique for image processing is The Fourier transform. In this work, the special feature for image quality (IQ) spectral comprises three parts. (i) arg (F) denotes phase (ii) Spectral Phase Error (SPE) (where F and $\hat{F}$ are the respective Fourier transforms of I and $\hat{I}$) (iii) Spectral Magnitude Error (SME).

5) Measure to be taken on a Gradient base

In the assessment of the quality of an image, one of the essential tools is Gradient. It provides the detailing of visionary information. There are types of distortion that can be corrected using a gradient. Mostly the information related to the structure and the changes in the contrast of the image can be easily identified and by applying the gradient difference can be significantly highlighted. The biometric protection system includes the two standard features of the gradient. (1) Gradient Phase Error (GPE) and (2) Gradient Magnitude Error (GME).

IV. SIMILARITY MEASURES BASED ON STRUCTURE

The quality of the scoring system based on subjective selection faces many difficulties in the old metrics of image quality. This represents the calculation of error sensitivity of mismatch in many cases. To assess the quality of the image, a newly developed sample having structural similarity was selected for the hypothesis: the first information received by the visual system is the dimensional view of the structural detail. Many reasons can distort images like changing the behavior of the light path and uneven patterns of the non-structural distortions which cover both the parts of contrast and brightness. Every distortion should be treated differently. Among the recent objective perceptual measures, the Structural Similarity Index Measure (SSIM) is the most straightforward developed concept that has been widely used in many practical applications. By observing the properties of SSIM, all 25 feature parameterizations have been included.

A. Measure based on Theoretical Information

Based on the theory perspective, the information related to the problem of quality assessment has signal fidelity. The mechanism working on the approach of communication of image source receives the information through a flow of channels which can limit the information by generating distortion. The target to maintain the quality of the test‘s image is to provide the appropriate precise piece of information to the test and the selected reference sample to develop coherence.

B. Types of Theoretical Information Features

In this study, two types of theoretical-based features are used: (1) Reduced Reference Entropic Difference Index (RRED) and (2) Visual Information Fidelity (VIF). These metrics have their perspective in IQA which has the qualities to approximate the local and global problem.

1. Reduced Reference Entropic Difference Index (RRED): The RRED metric deals with approaches to problems in QA. It measures the perspective amount of local information. The difference is generated between the reference image and the projection of the distorted image. To meet the criteria of wavelet domain sub-band, the difference is measured on the space of natural images. The algorithm of RRED can calculate the local entropies of distorted images and the local entropies Their average difference can easily be calculated in a distributed fashion.
2. Visual Information Fidelity (VIF): the ratio between the total original information in entropy and the distorted data of the image is measured by VIF metric. It conveys comprehensive data on the reference image completely. On the contrary, the RRED doesn’t need to get access to all the information of the reference image, even a small detail is essential to fulfilling the requirement.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

V. MEASURE TO BE TAKEN ON NO-REFERENCE IQ

The objective reference of the IQA methods is, the eye of the human body does not need any image quality parameter to set the standard. The principle is based on the automatic phenomenon to measure the no-reference image quality. The algorithm of (NR-IQA) has difficult and versatile parameters to assess the quality of the image if no reference sample is provided. The methods of NR-IQA mainly determine the quality parameter on the defined models of stats. The techniques are divided into one of the three trends based on the images used for training the present model and the requirement of prior knowledge [26].

A. Approaches of Specific Distortion

The specific distortion of the image causes the loss in visual quality by the techniques. In the study, the final sample of the model was calculated to measure the quality of the clean and the distorted images. The method of biometric protection has two measures in the present study. The quality of the images in JPEG is usually affected by the blocking object present in the low bits of the compressed algorithm. This is known as the JPEG Quality Index (JQI). On the contrary, there is a collection of literature representing the blind metrics to detect the parameter of blur and noise known as The High-Low Frequency Index (HLFI). It is also considered as the local gradients. The special feature of the HLFI is to correct sensitive details, such as the sharpness of the image. The other function is to compute the difference in the power of the upper and the lower frequencies of the Fourier Spectrum.

B. Training-based approaches

In NR-IQA methods, the model is used to implement the practices of clean and distorted images. Based on the computational quality score, different types of features of the images were extracted. The metrics of an image are provided by the availability of the former approaches in the quality score. To present the statistical model, there are many types of distortion models to affect the quality of the image. One example is the Blind Image Quality Index (BIQI), which can employ a 25-feature set to propose the model of the study. The model framework of the BIQI represents the system in two stages. This framework measures the capabilities of an individual to generate different kinds of distortion-specific experts on the level of one quality score.

C. Statistics Approaches Based on Natural Scene

The technique of blind IQA generally extracts information from natural scene distortion. In our study, the initial model is trained using natural scene distortion-free images, as outlined in Figure 2: Flow Diagram of the proposed technique. This methodology is rooted in the hypothesis that undistorted images encapsulate the regular properties of nature, falling within the associated subspace. The model functions by quantifying image quality, striving for accurate evaluation of natural image statistics for perceptual quality assessment. This method, initially proposed in the Natural Image Quality Evaluator (NIQE), is also employed in our current investigation. The model serves as a blind image quality analyzer, constructing features based on a statistical model aligned with the multi-variety Gaussian natural scene.

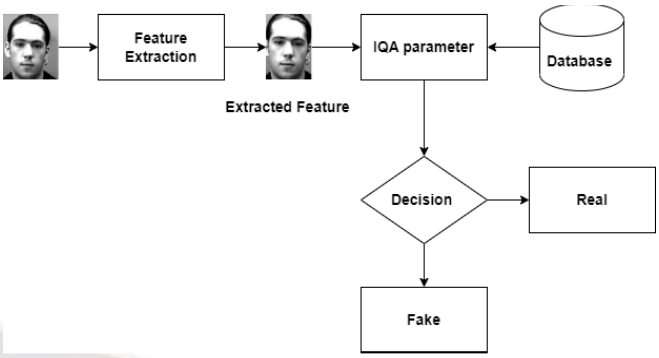

Figure 2. Flow Diagram of the proposed technique.

VI. ANALYSIS AND DISCUSSION

A. Quality Parameters

The study has considered various quality parameters such as; Peak Signal to Noise Ratio (PSNR), Correlation Factor, and Total Time Elapsed in Seconds.

- Peak-Signal to-Noise Ratio (PSNR): Peak-Signal to-Noise Ratio is used to determine the reconstruction of compression codecs with loss of quality. It is also known as image compression. It approximates reconstruction quality in the body. According to the study, there are many pieces of evidence in which one of the reconstructions developed to be like the original image. Even though it has a low PSNR, it usually requires a high PSNR quality. PSNR is expressed in the logarithmic decibel scale. It is mainly defined through MSE (mean square error). The PSNR is defined using Equation (1).

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (1)$$

  Where *MAXI* 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 number of rows and *n* is the number of columns.
- Mean Square Error (MSE): It calculates the average in the squares of the errors, to determine the estimator and estimated value difference. MSE is denoted by Equation (2).

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

- K Structural Content (SC): It calculates the ratio of the sum of the original image and the reference image and the square between them. SC is denoted by Equation (3).

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

- Average Difference (AD): The difference in the average estimated value for every pixel. That is the detraction of the original image from the reference image. AD is defined using Equation (4).

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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

- Normalized Absolute Error (NAE): The ratio between the sum of the absolute difference image and the absolute of the original image. This equation is referenced as Equation (5).

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

- Signal-to-Noise Ratio (SNR): The signal-to-noise ratio can be written as SNR or S/N. This is required in the field of business and science to maintain the proper signal level contrast associated with the noise level of the background. It is defined to calculate the ratio of the signal power to noise power and is represented in decibels. To indicate more signal than noise, the higher ratio is determined than 1:1 ($\geq$ 0 dB). The form of application of a signal to SNR is known as an electrical signal. According to the theory of Shannon–Hartley, the theorem is linked to the SNR, the degree of communication of the channel along with bandwidth. The signal-to-noise ratio does not recommend a ratio of useful information to false data in exchange. However, on online platforms, many societies and councils of conversation suggest junk as ”noise” which constrains the ”signal” in proper conversation.

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

- Maximum Difference (MD): The value of the maximum absolute difference image is determined. It defines the detraction of the original image from the reference image. This equation is presented using Equation (7).

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

- Structural Similarity index (SSIM): This image quality assessment is based on the computation of factors luminance (l), contrast (c), and structure (s). This equation is presented as:

$$SSIM\ (x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_xy+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (8)$$

- Measurement of Blind Image Quality Index (BIQI): This technique is used to train the alteration-free images from the natural scene with the help of the first model. It can do the tendency counts based on the hypothesis that explicit images of the world. It converts the natural images into the specific regular
- modification of all subspace images. The appropriate quantification can help to evaluate the statistics of the natural image and is able to develop an accurate perceptual quality.

B. Experimental Results

1) Result for Iris

This study compares the iris parameters of the input image with database information.

- The first sample: The biometric result obtained for Figure 3 is fake as shown in Table 1.

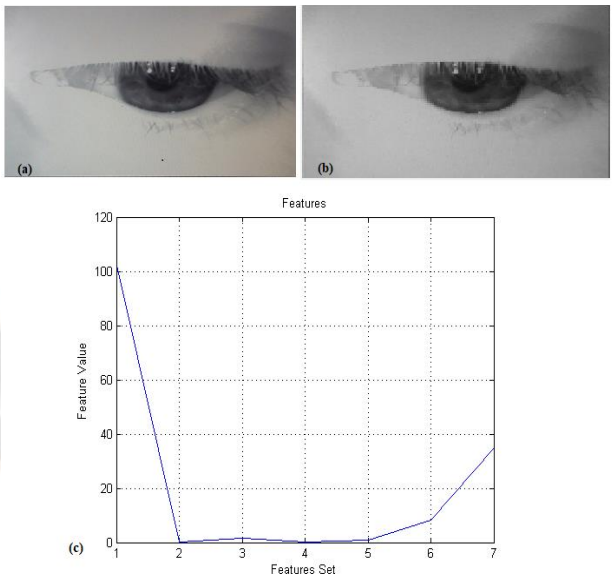

Figure 3. Result analysis of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

TABLE I. CALCULATION OF VALUES FOR DIFFERENT PARAMETERS.

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	95.74
2	Mean Square Error (MSE)	4.0869
3	Structural Content (SC)	1.00137
4	Average Difference (AD)	0.150274
5	Normalized Absolute Error (NAE)	0.000676
6	Signal-to-noise ratio (SNR)	28.1557
7	Maximum Difference (MD)	51
8	Training Based Measure (BIQI)	8.2524e-05

- The second sample: The biometric result obtained for Figure 4 is actual as shown in Table 2.

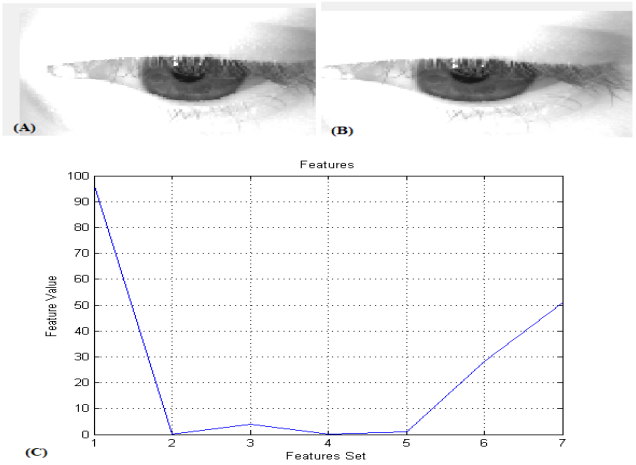

Figure 4. Result analysis of iris (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 September 2023* ***Revised:*** *12 November 2023* ***Accepted:*** *16 December 2023*

TABLE II. CALCULATION OF VALUES FOR DIFFERENT PARAMETERS.

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	97.985
2	Mean Square Error (MSE)	1.4996
3	Structural Content (SC)	1.00104
4	Average Difference (AD)	0.07995
5	Normalized Absolute Error (NAE)	0.00054
6	Signal-to-noise ratio (SNR)	8.10403
7	Maximum Difference (MD)	35
8	Training Based Measure (BIQI)	3.03668e-05

2) Result for Fingerprint

This study compares the thumb parameters of the input image with database information.

- The first sample: The biometric result obtained for Figure 5 is fake as shown in Table 3.

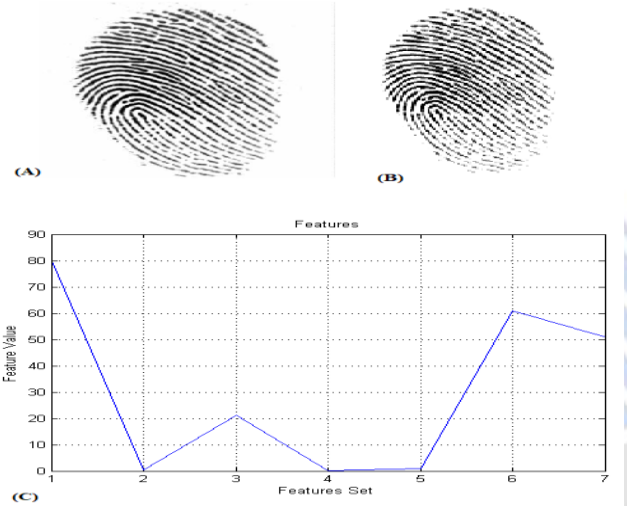

Figure 5. Result analysis of thumb (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

TABLE III. CALCULATION 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)	0.27814
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 second sample: The biometric result obtained for Figure 6 is actual as shown in Table 4.

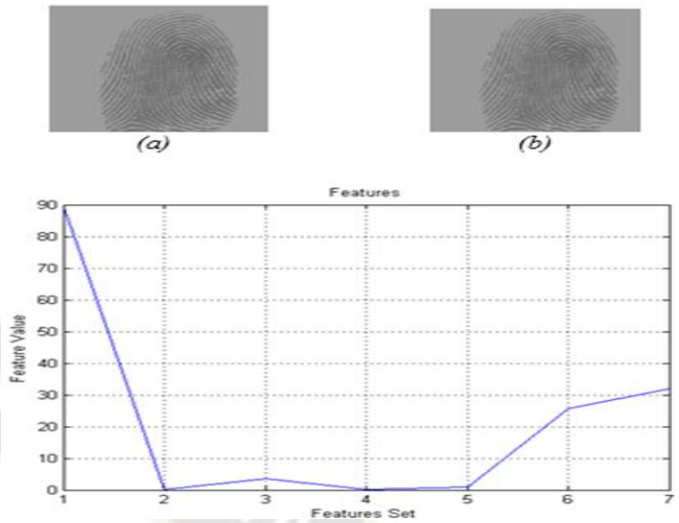

Figure 6. Result analysis of thumb (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

TABLE IV. CALCULATION 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)	0.001211
6	Signal-to-noise ratio (SNR)	25.6343
7	Maximum Difference (MD)	32
8	Training Based Measure (BIQI)	3.10663e-05

3) Result for Face Recognition

This study compares the face parameters of the input image with database information.

- The first sample: The biometric result obtained for Figure 7 is fake as shown in Table 5.

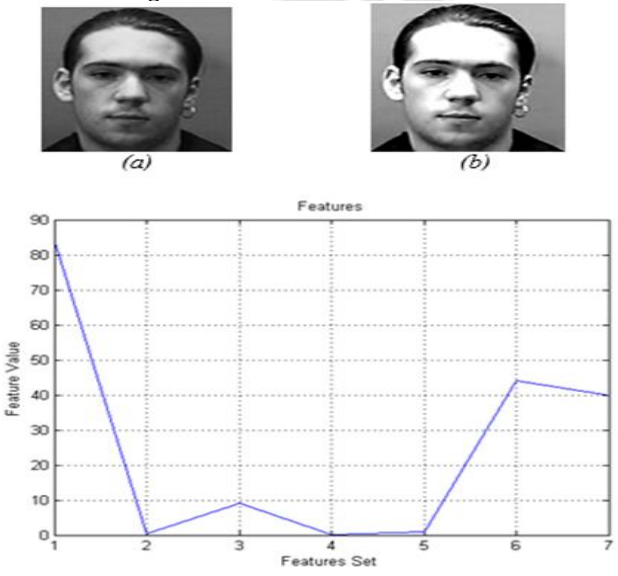

Figure 7. Result analysis of face (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 September 2023 **Revised:** 12 November 2023 **Accepted:** 16 December 2023*

TABLE V. CALCULATION OF VALUES FOR DIFFERENT PARAMETERS.

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	84.1888
2	Mean Square Error (MSE)	9.09325
3	Structural Content (SC)	1.00802
4	Average Difference (AD)	0.40075
5	Normalized Absolute Error (NAE)	0.002366
6	Signal-to-noise ratio (SNR)	44.1506
7	Maximum Difference (MD)	40
8	Training Based Measure (BIQI)	04.11243e-05

- The second sample: The biometric result obtained for Figure 8 is actual as shown in Table 6.

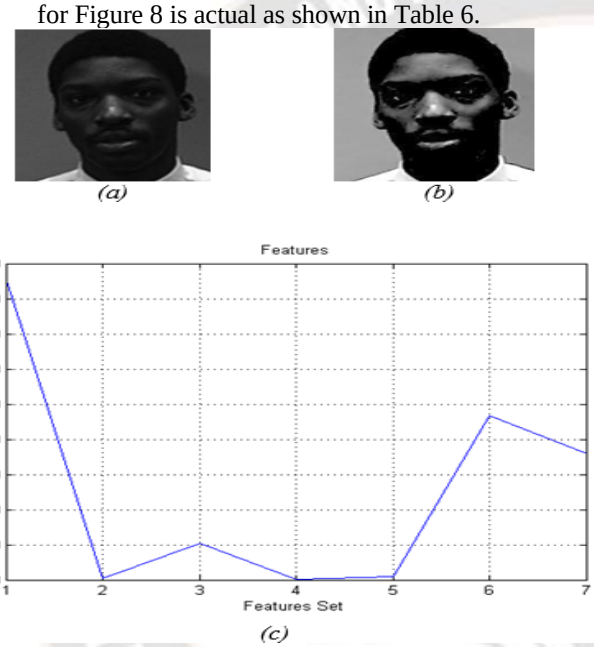

Figure 8. Result analysis of face (a) Input Image (b) Gaussian image (c) Graphical representation of Quality Parameters.

TABLE VI. CALCULATION OF VALUES FOR DIFFERENT PARAMETERS.

Sr. No.	Parameter	Value
1	Peak Signal to Noise Ratio (PSNR)	85.6073
2	Mean Square Error (MSE)	8.3952
3	Structural Content (SC)	1.00572
4	Average Difference (AD)	0.325806
5	Normalized Absolute Error (NAE)	0.002703
6	Signal-to-noise ratio (SNR)	43.8269
7	Maximum Difference (MD)	36
8	Training Based Measure (BIQI)	0.00304596

4) Performance Comparison

Table 7 presents the comparison of PSNR for the proposed technique, Gull et al. technique [27], Trivedy and Pal's technique [28], and Bal et al.'s technique [29]. The proposed technique and Gull et al.'s (2020) technique produce almost identical results as the average PSNR is 89.04.

TABLE VII. AVERAGE RESULTS OF PSNR FOR THE PROPOSED TECHNIQUE, GULL ET AL.'S TECHNIQUE, TRIVEDY AND PAL'S TECHNIQUE, AND BAL ET AL.'S TECHNIQUE.

	Proposed technique	**[27]**	**[28]**	**[29]**
	PSNR	PSNR	PSNR	PSNR
Avg.	89.08	51.13	51.06	34.41

VII. CONCLUSION

This paper presents the new structural and institutional flow map of the biometric system which can easily fulfill the requirement of quality and security of any organization of big and small-mid enterprises. Furthermore, more extensions can be provided in this model framework. The method to determine the evaluation of image quality is by creating the difference between original and fake images. This helps the security system to become strong and create authenticity. It provides support to the multi-biometric and assures the quality framework of the multi-assault model. This idea can be expanded to many other platforms. By looking at all the parameters, it provides a proficient outcome. With novel programming and image quality appraisal, it gives a quick reaction.

A new technique is executed for various biometric modalities like iris, fingerprint, and face utilizing a publicly accessible database. A Biometric recognizable proof framework gives a precise outcome. Likewise, programming and equipment are easy to use without additional pieces of establishment and treatment of framework. It finishes its activity in a few seconds, so it is efficient. This framework is utilized for offices or different applications for login reasons. The biometric framework is advantageous in providing security arrangements since the client cannot require ID confirmation. This watchword is hard to deal with consistently for the login framework.

REFERENCES

[1] A. Kaushik, The usage of technology by the senior citizens: Opportunities and challenges, Evolution of Digitized Societies Through Advanced Technologies (2022) 75–85.
[2] J. Galbally, S. Marcel, J. Fierrez, Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition, IEEE transactions on image processing 23 (2) (2013) 710–724. 25
[3] S. Kumar, M. D. Ansari, M. V. Naik, V. K. Solanki, V. K. Gunjan, A comparative case study on machine learning based multi-biometric systems, Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies (2020) 353–365.
[4] S. Arora, M. Bhatia, Challenges and opportunities in biometric security: A survey, Information Security Journal: A Global Perspective 31 (1) (2022) 28–48.
[5] K. Gupta, G. S. Walia, K. Sharma, Quality based adaptive score fusion approach for multimodal biometric system, Applied Intelligence 50 (2020) 1086–1099.
[6] P. S. Prasad, R. Pathak, M. Janga Reddy, V. K. Gunjan, Analyzing correlation based matching in biometric system, in: ICCCE 2019: Proceedings of the 2nd International Conference on Communications and Cyber Physical Engineering, Springer, 2020, pp. 413–418.
[7] A. K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on circuits and systems for video technology 14 (1) (2004) 4–20.
[8] Z. Sun, A. A. Paulino, J. Feng, Z. Chai, T. Tan, A. K. Jain, A study of multibiometric traits of identical twins, in: Biometric technology for human identification Vii, Vol. 7667, SPIE, 2010, pp. 283–294.

[9] Y. Kortli, M. Jridi, A. Al Falou, M. Atri, Face recognition systems: A survey, Sensors 20 (2) (2020) 342.
[10] J. Galbally, C. McCool, J. Fierrez, S. Marcel, J. Ortega-Garcia, On the vulnerability of face verification systems to hill-climbing attacks, Pattern Recognition 43 (3) (2010) 1027–1038.
[11] S. M. Meena, A. B. Nandurbarkar, A literature review on liveness assessment of multimodal biometrics through image quality assessment.
[12] P. M. Shende, M. V. Sarode, M. M. Ghonge, A survey based on fingerprint, face and iris biometric recognition system, image quality assessment and fake biometric, International Journal of Science, Engineering and Computer Technology 4 (4) (2014) 129.
[13] V. K. Gunjan, P. S. Prasad, R. Pathak, A. Kumar, Machine learning methods for extraction and classification for biometric authentication, ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications, Springer, 2020, pp. 1984–1988.
[14] J. Zhou, Y. Wang, Z. Sun, Y. Xu, L. Shen, J. Feng, S. Shan, Y. Qiao, Z. Guo, S. Yu, Biometric Recognition: 12th Chinese Conference, CCBR 2017, Shenzhen, China, October 28-29, 2017, Proceedings, Vol. 10568, Springer, 2017.
[15] Y. Jiang, X. Liu, Spoof fingerprint detection based on co-occurrence matrix, International Journal of Signal Processing, Image Processing and Pattern Recognition 8 (8) (2015) 373–384.
[16] S. Chinthu, C. Dhanabal, Fake identification in fingerprint, iris and face recognition using image quality assessment.
[17] M. R. Ramachandran, Spoofing protection for biometric systems.
[18] M. Sepasian, C. Mares, W. Balachandran, Liveness and spoofing in fingerprint identification: Issues and challenges, in: Proc. 4th WSEAS Int. Conf. Comput. Eng. Appl.(CEA), 2009, pp. 150–158.
[19] B. Fu, F. Kirchbuchner, N. Damer, The effect of wearing a face mask on face image quality, in: 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021), IEEE, 2021, pp. 1–8.
[20] B. Fu, C. Chen, O. Henniger, N. Damer, A deep insight into measuring face image utility with general and face-specific image quality metrics, in: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2022, pp. 905–914.
[21] S. Lyu, H. Farid, Steganalysis using higher-order image statistics, IEEE Transactions on information Forensics and Security 1 (1) (2006) 111– 119.
[22] M. C. Stamm, K. R. Liu, Forensic detection of image manipulation using statistical intrinsic fingerprints, IEEE Transactions on Information Forensics and Security 5 (3) (2010) 492–506. 27
[23] J. Galbally, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, A high performance fingerprint liveness detection method based on quality related features, Future Generation Computer Systems 28 (1) (2012) 311– 321.
[24] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, IEEE transactions on Image Processing 12 (2) (2003) 221–229.
[25] S. Bayram, ˙I. Avcıba¸s, B. Sankur, N. Memon, Image manipulation detection, Journal of Electronic Imaging 15 (4) (2006) 041102–041102.
[26] M. A. Saad, A. C. Bovik, C. Charrier, Blind image quality assessment: A natural scene statistics approach in the dct domain, IEEE transactions on Image Processing 21 (8) (2012) 3339–3352.
[27] S. Gull, N. A. Loan, S. A. Parah, J. A. Sheikh, G. M. Bhat, An efficient watermarking technique for tamper detection and localization of medical images, Journal of ambient intelligence and humanized computing 11 (2020) 1799–1808.
[28] S. Trivedy, A. K. Pal, A logistic map-based fragile watermarking scheme of digital images with tamper detection, Iranian Journal of Science and Technology, Transactions of Electrical Engineering 41 (2017) 103–113.
[29] S. N. Bal, M. R. Nayak, S. K. Sarkar, On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching, Journal of King Saud University-Computer and Information Sciences 33 (5) (2021) 552–561.