iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49513

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Biometrics: An Evolving Industry with Unique Risks

Harkesh Prajapati[1], Abhijeet Singh[2], Bhaskar Mishra[3], Dr. Richa Vijay[4]
[1, 2, 3, 4]*Department of Computer Applications, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana*

Abstract: ***Biometrics is a cutting-edge technology that offers several advantages for access privileges and authorization. This security system has become an integral part of a variety of public and commercial sectors. The importance of growing private data for authentication solutions that increase mobile security is rising. Information security is required to prevent organisations' assets from falling into the hands of rivals, hackers, or cyberterrorists. This study explains how to avoid the biometric methods' concealed dangers. Compared to traditional systems, biometric applications are capable of providing much more identity management and recognition. In truth, the widespread use of biometrics services has substantial consequences for our understanding of the relationship between the person and the state. As with any technology, however, application-specific concerns and limitations must be taken into account. Research in a number of connected fields will lead to continuing progress. In this study, technical and engineering challenges as well as the advantages of contemporary biometric technology are examined.***

Keywords: biometrics, access privileges, eigenface, fingerprint, iris, voice.

I. INTRODUCTION

Biometrics comes from the words bio, which means life, and matron, which means measurement. Hence, identification/ authentication is achieved by measuring some inherent characteristics of the user. The process of using user-specific characteristics to verify that a user has logged into an account, accessed personal information, etc. Fingerprint scans, facial images, signatures, voice recognition, and biometrics. If the user is already registered or if the user data has already been registered in the system software, identity verification will take place. In this case, the input data provided by the user is compared with previously provided input data. Physiological or behavioural traits that match already registered traits can be found, logged in and stored for future use. This system offers much higher reliability than traditional PINs or other ID or document-based systems. Several sectors, including law enforcement, government, banking, healthcare, and consumer devices, have seen an increase in the use of biometrics. Compared to conventional identification techniques like passwords or tokens, biometric verification has many benefits, including increased security, ease of use, and quickness. But there are also particular problems with biometric devices, like accuracy, anonymity, and data security.

II. RESEARCH OPPORTUNITIES

Numerous research problems in biometric systems and technology have presented significant obstacles to this sector in recent years. In recent years, biometrics has emerged as a financially successful solution, and as it continues to develop, it will undoubtedly have a profound impact on our everyday lives. The truth has been skewed, nevertheless, by myths regarding the technological, functional, and societal implications of biometric systems. The most prevalent biometric IDs and conventional biometric systems are covered in this section.

A. Face Recognition

Face detection is among the biometric techniques that is thought to be the least invasive since we constantly rely on differentiating face features to tell people apart. Our visual cortex must synthesise the many sources of information into usable patterns while our brain's specialised nerve cells react to certain local aspects. Extracting relevant features, displaying those features, and finally classifying them are all steps in automated recognition. Global or regional image encoding is an option. Local models are based on determining the connection between several face characteristics, such as the distance between the eyes or between each eye and the nose, etc. Like the eigenface technique, the global model is template-based. The common subset of these Eigenfaces may be thought of as the basis for any human face. One method, fisherfaces, is supposed to be less susceptible to variations in lighting and facial angles. Each Eigenface indicates a pattern of evaluation of many facial traits.

Even one to three day old neonates can recognise familiar faces, making face identification a simple task for people.[16] Questions about how to assess a picture and how the brain encodes information as well as whether to use inner or outside characteristics for successful face recognition have been raised. Segmentation, which separates face traits from background data, offers ongoing prospects for facial identification.[10,11]

Standard optical scanners may be used to take still pictures and real-time video for image capture. Some more recent systems employ stereo, structured light, or phase-based ranging to create a 3D picture of the face, and near infrared can be added to face detection in low-light situations.[14,17]

Lack of appropriate training samples, uncontrolled variables, or volatility in the circumstances may prevent the matcher from accurately modelling the invariance relationship, which will lead to low matching accuracy.[2]

B. Fingerprint

The first biometric system that has been successfully used in daily life is fingerprint-based identification. The fingerprint is the most widely used biometric for law enforcement, border control, and individual identification verification. It is believed that the fingerprint's ridge and furrow patterns, as well as the ridge characteristics present at either a ridge bifurcation or a ridge ending—the so-called minutiae points—represent its invariable and permanent nature. Image or correlation techniques, minutiae-based approaches, and hybrid or ridge feature-driven methods are the three most common ways of representing and matching fingerprints in the literature. For sensed measurements to be invariant, an optimal representation should be created. The ability to distinguish between photos is limited by the low quality images that cannot be processed by a regular fingerprint recognition system.

The image resolution quality offered by the scanner must be taken into account while taking a fingerprint image. Variations in picture quality affect the kind and range of characteristics that may be used for analysis. The need that the user contact the scanning device while enrolling or authenticating is another distinctive feature of fingerprint biometrics. Artifacts may accumulate on the platen in the form of natural skin oil smudges and grime, or they may scrape the platen as a consequence of contact. Therefore, there is a lot of variation among different impressions of the same finger due to scanner quality (pixel intensity) and usage. This is known as a high intra-class variance in representational terms, meaning that different pictures of the same finger may appear.[4,7]

On the other hand, photos from several fingers tend to seem very similar when there is not much inter-group diversity. Finding a quantifiable feature space that permits clustering of photographs of the same digit while images for other fingers inhabit a distinct part of the space is suitable for achieving minimal intra-class variance (high inter-class variation).[15]

As a result, ideal matching implies that there should be a small gap in the feature space between two representations of the same finger. This implies that there should be a high degree of resemblance between them. In other words, the representation methodology's features should, to the greatest extent feasible, be immune to the major issues caused by intra-class variance. In an effort to address the primary shortcomings of both local and global representation strategies, ridge feature-based approaches are a mix of the two. Insufficient quality fingerprint photos may make it difficult to retrieve local details. More reliably than minutiae, other characteristics of the ridge pattern, such as its direction, frequency, and texture information, may be retrieved.[5]

Understanding specific modes and how to deploy them efficiently is crucial to the system's overall performance. Reduce enrollment (FTE) and failure to acquire (FTA) rates, ideally by the development of innovative sensors. Artefact recognition, image quality definition and improvement, and high-resolution fingerprint matching are a few particular fingerprint-related difficulties..[20]

C. Iris

Iris patterns are both mathematically and aesthetically unique due to their complexity and their inherent randomness. In addition to its colour, the iris may be identified by its ligaments, furrows, ridges, crypts, rings, corona, and freckles. The concept of using the iris as a biometric has been around for over a century. Dr. John Daugman of Cambridge University's computer laboratory created the primary algorithms for picture capture, feature extraction, and matching in 1994 and provides a thorough discussion of the technical and performance aspects of his methods.[9]

The inadequate accuracy performance of biometric systems is mostly due to information restriction, representation limitation, and invariance limitation. Due to the intrinsic signal capacity of biometric identification, pattern samples containing unique and invariant information may be limited. The absence of information may be attributable to the acquisition of unsupervised, controlled signals. Iris recognition systems provide opportunities for research and development in the following areas: sensors; optimization of the light spectrum; decrease of FTE and FTA rates; recording and identification of the iris at greater distances and subject motion; and hardware size reduction.

Acquiring high-quality eye photos in less-than-ideal settings and accurately recognising the iris' spatial extent in low-quality photographs are two challenges that need to be addressed if researchers are to keep up the progress achieved in iris recognition over the last decade. The intricacy of iris patterns and their expected stability, however, provide a powerful incentive to address these issues and broaden the scope of iris recognition applications.

Low-quality iris video pictures are swiftly weeded out by the video-based image processing methods. Blurring caused by defocus, blurring caused by motion, off-angle viewing, occlusion, specularity, illumination, and pixel counts are all taken into account to determine the final picture quality. The Dempster-Shafer method incorporates computed individual factors into an overall quality evaluation. Using the quality measure as a predictor of recognition accuracy is shown. An initial segmentation is needed for the calculation of the quality measure; hence, poor localization or segmentation will lead to erroneous quality ratings.

To remove iris image anomalies, appropriate global enhancement functions are applied to the iris image input. While these methods increase the quality of low-resolution image regions, they also modify the characteristics of acceptable or high-resolution image regions. In addition, the poor quality of a photograph may be caused by a number of anomalies, such as when there is an abundance of noise, not enough light, or motion artefacts caused by the capturing process.

To enhance these images, it is important to segment the afflicted regions locally and apply the appropriate improvement algorithms. There have been a number of segmentation techniques for iris pictures to far. However, no currently available technique for iris segmentation can guarantee 100% accuracy. An iris segmentation evaluation method is necessary to improve the accuracy of iris identification. As recognition systems are deployed to bigger populations, the requirement to reduce complexity via encoding and optimise matching algorithms will grow. How to integrate several images to enhance performance, as well as how to improve recognition for people who use glasses, are two more areas that have not received a lot of attention.[8]

D. Voice

The human voice is a convenient biometric for many people and the only biometric choice for the vast bulk of existing audio-based technologies. Remember that speech recognition is different from speaker verification (or recognising a specific speaker) (i.e. identifying what is being said). Unlike passwords and keys, which can be easily forgotten or lost, speech biometrics are a permanent form of security. Historically, spectrograms were used to determine the speaker's identity. This strategy, however, was fraught with issues and obstacles. Automatic speaker identification is proposed as a means of overcoming the drawbacks of prior techniques. characteristics are retrieved from speech samples prior to modelling and storing the samples in a speaker database. When matching is needed for speaker identification, characteristics are retrieved from speech samples and compared with a database. On the basis of this match, the sample is either accepted or rejected.

Typically, speaker identification systems must convert collected analogue voice signals to digital before applying spectral analysis concepts to them. The ceptstral feature vector used to represent the human voice may be extracted via Fourier transforms, which can be utilised to produce coefficients for complex audio wave functions. Over the last four decades, researchers have used both behavioural and anatomical traits to successfully identify speakers. A person's speaking manner, voice pitch, and timbre are all learned behaviours, but physical traits like the size and shape of one's vocal cords, vocal tract, and palate all play a role in one's voice. Speaker system templates, often known as "voice prints," integrate behavioural and physical traits, hence the method may be categorised as a behavioural biometric. The widespread use of cellphones and other auditory devices makes speaker identification a desirable safety precaution.

Separating voices, standardising channels, and relying on more refined information may all improve the accuracy of speaker identification. It's possible that needing traits like toughness and persistence might help improve voice recognition. Because of the rapid pace of linguistic and behavioural changes, as well as the dearth of available speech samples, researchers must be resilient and persistent in their efforts. There is a long way to go before real-time speech identification is fully functional. A digital signal processor (DSP) might be used to accomplish speaker identification.[1,3]

III. FACTORS OF THREAT LINKED TO BIOMETRIC IDENTIFICATION

Most biometrics systems do not encrypt or hash user data, allowing for quick retrieval. A high FAR product owing to low-quality components may result in verifying the incorrect person, and tampering with the sensor or database can result in adding a person who should not be confirmed, both of which can make the system useless[19]. At the same time, a user's information that has already been entered into the system may be replicated and delivered in a number of different forms. It's analogous to using a photo two-dimensional face recognition. Because of bugs in the Face ID technology, children and even identical twins have sometimes been able to unlock the newest iPhone[12].

The sensor used to authenticate the device may be compromised if an adversary had physical access to it[18].Communication channels between system components are vulnerable to attacks such as man-in-the-middle attacks, brute-force attacks, re-authentication of obtained data, and the fabrication of bogus data for matching. Access to the database endangers the privacy and security of the stored information. The ability to read unencrypted data might lead to the disclosure of sensitive information. Changes to the identity-biometric link might render authentication useless. If it is possible to make decisions and match values, it is also possible to change the input value's degree of matching, re-enter the value, verify the match results, and launch brute-force attacks. Further, automatic and unsupervised registration in biometric identification systems is always vulnerable to identity fraud. False or misleading information provided during registration might lead to identity theft or a false biometric match. Despite these risks, ensuring the system's physical security is the most important security measure. Data in a database has to be either stored or encrypted simultaneously. Inter-component traffic flows are useful for fixing channel problems. Unfortunately, the performance of the gadget will be hindered by all of these features (or system). Even at machine speed, each encryption operation might increase the time necessary for authentication. Nevertheless, such procedures should be adopted when security and identification assurance are required. Due to the issues inherent with biometric authentication, it is also suggested that biometric verification be used as a supplementary approach, rather than as the only one.

IV. RISK ASSESSMENT AND REDUCTION METHODS

Risk assessment is a crucial component of any intelligent technological systems that must address issues. An evaluation of risk is conducted to ascertain how probable and severe prospective threats are. Biometric systems face two distinct types of threats: hackers and non-hackers (human errors, structural failures, or natural disasters). By examining the outcome, you may determine the likelihood and severity of an assault. To make an informed choice, you must be aware of the process's inherent risk. In the essay by Pokorádi, a research on risk assessment using fuzzy logic is presented.[13]

There are a range of methods for ensuring that biometrics are utilised correctly and minimising the risk connected with their usage. Encrypting and securing templates saved in databases from attackers is the first step. Consequently, digital scales may be used as encryption keys until they are used. Using the watermark technique, which involves the addition of additional data to the security object, security and authentication may be achieved. This addition of extra bits assures the source object's security. On the other hand, there is some distortion introduced by the source itself. With the watermarking method, supplementary database information (data source, data destination, etc.) is embedded into the data in a way that can be seen by the naked eye or not (image, sound, etc.). In biometrics, a watermark is used to verify the originality of the data and spot any alterations. Many biotechnologies, such as fingerprinting and iris scanning, might be integrated with models and sensors to greatly lower hazards. Adding extra biometric picture samples into the mix will slow down the validation process because of the additional math that will be required.[6]

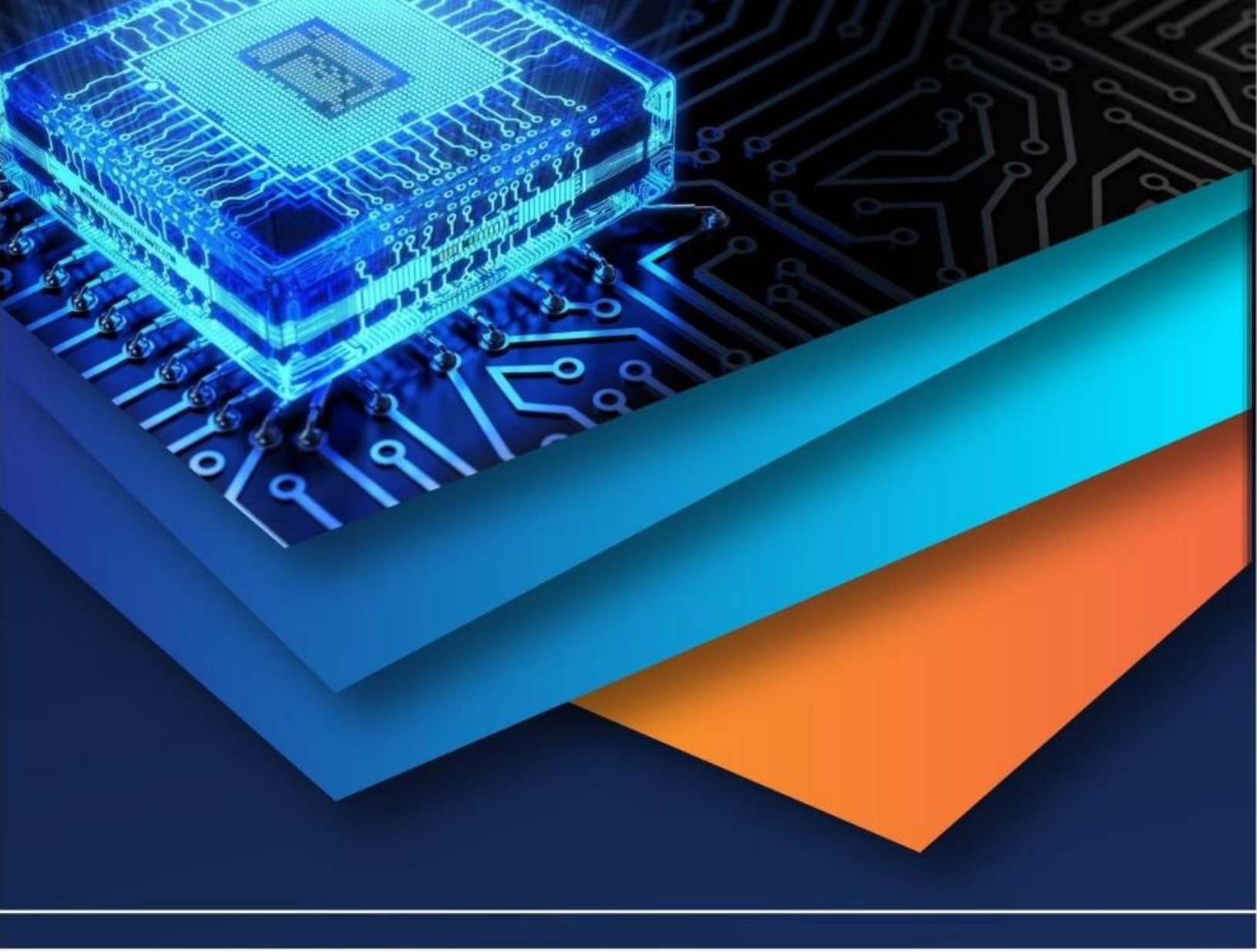
V. CONCLUSION

In this article, the authors provide a concise overview of the hidden dangers of biometric methods, as well as risk mitigation tactics and the two most prominent biometric technologies: fingerprint identification and face recognition. System security, system integrity, and system reliability are some of the security problems associated with biometric systems. In order to protect biometric systems against assaults based on the supply of fake biometrics, the reuse of previously obtained biometric samples, and the development of technologies, further study is needed in the field of information security. The biometric problem is not totally addressed, and the accuracy of present biometrics systems is not faultless, despite the fact that reliable personal recognition is necessary for a variety of commercial operations. Unique research topics include sensors and novel characteristics, prominent portrayal, effective pairing, different biometrics systems, and soft biometrics. Lack of uniqueness in biometric characteristics, mistaken identification, administrative/insider attack, unsecured infrastructure, and lack of security are some disadvantages of biometrics systems. It may be essential to compromise between security and privacy. Future scope is considered and studied for technical and engineering domains resulting from prolonged study.

REFERENCES

[1] Mandeep Singh Walia, 2015, “Modern Biometric Technologies: Technical Issues and Research Opportunities”, viewed on November 15, 2022, available at: https://www.iosrjournals.org/iosr-jece/papers/AETM%2715_ECE/02-ECE-122.pdf
[2] Electronic Frontier Foundation, 2017, “Street-Level Recognition”, viewed on November 15, 2022, available at: https://www.eff.org/pages/face-recognition
[3] Biometric Solutions, 2016, “Biometrics”, viewed on November 15, 2022, available at: https://www.biometric-solutions.com
[4] Biometric Solutions, 2016, “Fingerprint Recognition”, viewed on November 16, 2022, available at: https://www.biometric-solutions.com/fingerprint-recognition.html

[5] Mark Clark, Danny Thakkar, 2022,"Fingerprint Identification: Reference Point Detection and Feature Extraction", viewed on November 16, 2022, available at: https://www.bayometric.com/fingerprint-reference-point-detection-and-feature-extraction/
[6] Haya Altaleb, Sinan Kocak, 2019, "The Risk of Using Biometrics", viewed on November 16, 2022, available at: https://www.researchgate.net/publication/332079038_The_Risk_of_Using_Biometrics
[7] Neil Yager, Adnan Amin, 2004, "Fingerprint Verification Based on Minutiae Features: A Review", viewed on November 17, 2022, available at:
[8] https://www.researchgate.net/publication/220654559_Fingerprint_verification_based_on_minutiae_features_A_reviewZhi Zhou, Yingzi Du, Craig Belcher, 2009, "Transforming Traditional Iris Recognition Systems to work in Nonideal Situations", viewed on November 17, 2022, available at: https://www.researchgate.net/publication/224503995_Transforming_Traditional_Iris_Recognition_Systems_to_Work_in_Nonideal_Situations
[9] John G. Daugman, 1993, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", viewed on November 18, 2022, available at: https://www.cl.cam.ac.uk/~jgd1000/PAMI93.pdf
[10] Matthew Turk, Alex Pantland, 1991, "Eigenfaces for Recognition", viewed on November 18, 2022, available at: https://doi.org/10.1162/jocn.1991.3.1.71
[11] Peter N. Belhumeur, Joao P. Hespanha, and David J. Kriegman, 1997, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", viewed on November 19, 2022, available at: https://cseweb.ucsd.edu/classes/wi14/cse152-a/fisherface-pami97.pdf
[12] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, 2015, "Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption", viewed on November 19, 2022, available at: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4969 HYPERLINK "https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4969&context=sis_research"& HYPERLINK "https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4969&context=sis_research"context=sis_research
[13] Laszlo Pokoradi, 2002, "Fuzzy logic-based risk assessment", viewed on November 19, 2022, available at: https://uni-obuda.hu/users/pokoradi.laszlo/02_b.pdf
[14] Jaiswal Sushma, Sarita Singh Bhadauria, Rakesh Singh Jadon, Tarun Kumar Divakar, 2010, "Brief Description of Image Based 3D Face Recognition Methods", viewed on November 20, 2022, available at: https://doi.org/ HYPERLINK "https://doi.org/10.1007/3DRes.04(2010)02"10.1007/3DRes.04(2010)02
[15] Christoph Busch, Claudia Nickel, Chris Stein, Raghu Ramachandra, Kiran Raja, Pankaj Wasnik, Martin Stokkenes, Marta Gomez-Barrero, Andreas Nautsch, Christian Rathgeb, Ulrich Scherhag, John Ellingsgard, Martin Olsen, Carsten Gottschlich, Ctirad Sousedik, 2017, "Biometric Systems and Presentation Attacks", viewed on November 20, 2022, available at: https://www.christoph-busch.de/files/Busch-PAD-in-biometrics-ICCST-171025.pdf
[16] Aras Asaad, Sabah Jassim, 2017, "Topological Data Analysis for Image Tampering Detection", viewed on November 21, 2022, available at: http://bear.buckingham.ac.uk/397/1/TDA.pdf
[17] Bernhard Preim, Alexandra Baer, Douglas Cunningham, Tobias Isenberg, Timo Ropinski, 2016, "A Survey of Perceptually Motivated 3D Visualization of Medical Image Data", viewed on November 21, 2022, available at: https://doi.org/10.1111/cgf.12927
[18] Luiz Souza, Luciano Oliveira, Mauricio Pamplona, Joao Papa, 2018, "How far did we get in face spoofing detection?", viewed on November 21, 2022, available at: https://repositorio.unesp.br/bitstream/handle/11449/160335/WOS000434239000031.pdf;jsessionid=468DE803DCC47EF614BD963D60091101?sequence=1
[19] Danny Thakkar, Mary Clark, 2022, "False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics" viewed on November 22, 2022, available at: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/
[20] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, 2009,"Handbook of Fingerprint Recognition" viewed on November 23, 2022, available at: https://download.e-bookshelf.de/download/0000/0079/95/L-G-0000007995-0002341237.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY