



REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Information Technologies

**A NEW BIOMETRIC SYSTEM BASED IRIS
IMAGE ANALYZING USING CONVOLUTIONAL
NEURAL NETWORK**

Huda Adnan Hasan AL-SHAMMAERI

Master's Thesis

Supervisor

Asst. Prof. Dr. Ayça Kurnaz TÜRK BEN

Istanbul, 2023

**A NEW BIOMETRIC SYSTEM BASED IRIS IMAGE ANALYZING
USING CONVOLUTIONAL NEURAL NETWORK**

Huda Adnan Hasan AL-SHAMMAERI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled “ A NEW BIOMETRIC SYSTEM BASED IRIS IMAGE ANALYZING USING CONVOLUTIONAL NEURAL NETWORK” prepared by HUDA ADNAN HASAN AL-SHAMMAERI and submitted on 07/08/2023 has been **accepted unanimously** for the degree of Master of Science in Information Technology .

Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Supervisor

Thesis Défense Committee Members:

Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Department of Software

Engineering,

Altınbaş University

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Department of Computer

Engineering

Altınbaş University

Asst. Prof. Serdar KARGIN

Department of Biomedical

Engineering

Arel University

I hereby declare that this thesis meets all format and submission requirements of a Master’s thesis.

Submission date of the thesis to Institute of Graduate Studies: 2023_/08_/ 07_

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Huda Adnan Hasan AL-SHAMMAERI

Signature

PREFACE

I extend my sincere gratitude to my supervisor, Dr. Ayça Kurnaz TÜRKBEN, for her academic guidance at every stage of the dissertation. I am honored to be one of her students. I would also like to express my thanks to the members of the committee for their academic comments and for attending my dissertation defense session. Finally, I would like to express my sincere love and gratitude to my family for being their first supporter of my studies, especially my mother for her love and support for me in all stages of my life and her prayers for success and permanent excellence. Last but not least, special thanks to my manager at work, Engineer Muthanna Mahmoud Al-Tamimi, who was credited for my success in my academic career.

ABSTRACT

A NEW BIOMETRIC SYSTEM BASED IRIS IMAGE ANALYZING USING CONVOLUTIONAL NEURAL NETWORK

AL-SHAMMAERI, Huda Adnan Hasan

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Date: 08/2023

Pages: 80

Biometric systems are applying personal features to validate or identify a person. A system collects biometric characteristics unique to every person. These biometric characteristics are then directly linked to verify or identify the individual.

In this study new structure of CNN applied to classify IRIS images to recognize the persons. The proposed structure consist from 9 CNN features extraction layers which lead to decrease the size of input images and wired the extracted features to the classifiers such as ANN, MLP, RF, and DT. The presented results show that the proposed CNN based RF method presented best accuracies than other classifiers.

Keywords: CNN, Deep Learning, IRIS Images, MLP, DT.

TABLE OF CONTENTS

	<u>Pages</u>
ABSTRACT	vi
LIST OF TABLES.....	x
LIST OF FIGURES.....	xi
ABBREVIATIONS.....	xii
1. INTRODUCTION	1
1.1 FINGERPRINT RECOGNITION.....	3
1.2 HAND GEOMETRY	4
1.3 FACE RECOGNITION	4
1.4 IRIS RECOGNITION	5
2. OVERVIEW.....	7
2.1 SURVEY	7
2.1.1 Denial of Service Attacks (DoS) Message.....	10
2.1.2 Crime Control and Administrative.....	12
2.1.3 Control and Surveillance of Working Life	13
2.1.4 Consumption and Consumer Surveillance	13
2.1.5 Digital Tracking	16
2.1.6 Industry 4.0 and Smart, Integrated Systems	17
2.1.7 Web 2.0 and Cloud Computing	18
2.1.8 Big Data Analytics and Information	19
2.1.9 Combining the Eye with Artificial Intelligence and Biometric	20
2.1.10 New Payment Systems and Social Rating.....	22
2.1.11 Digital State and Digitization of the Individual	23

2.1.12 Digital-Based Surveillance Methods of the Individual	24
2.1.13 Individual's Interview Traffic Surveillance	25
2.1.14 Movement of the Individual, Location Surveillance	26
2.1.15 Written Interview Surveillance of the Individual	26
2.1.16 Individual Tendency, Lifestyle Surveillance	26
2.1.17 Digital Dictatorship.....	27
2.1.18 Immigrants	29
3. MATERIAL AND METHODS	41
3.1 APPLICATIONS OF BIOMETRIC SYSTEMS	41
3.1.1 Border Tracking and Surveillance	41
3.1.2 Information System.....	42
3.1.3 European Dactyloscopy Database (Eurodac).....	42
3.1.4 Ground Observation.....	45
3.1.5 Travel Information and Authorization System	47
3.2 CONVOLUTIONAL NEURAL NETWORKS	53
3.2.1 Fundamental Components of Convolutional Neural Networks	54
3.3 PROPOSED BIOMETRIC SYSTEM USING CNN	57
4. RESULTS	59
4.1 MMU IRIS DATASET	59
4.1.1 CNN Based Decision Tree Results with MMU IRIS Dataset	59
4.1.2 CNN Based Random Forest Results with MMU IRIS Dataset	60
4.1.3 Neural Network Results.....	61
4.1.4 MLP Results.....	62
4.2 CASIA-IRIS DATASET.....	63

4.2.1 CNN Based Decision Tree Results with CASIA-IRIS Dataset	63
4.2.2 CNN Based Random Forest Results	64
4.2.3 Neural Network Results	64
4.2.4 MLP Results.....	65
5. CONCLUSIONS	66
REFERENCES	67



LIST OF TABLES

Pages

Table 4.1: Comparison Previous Studies.....65



LIST OF FIGURES

	<u>Pages</u>
Figure 1.1: Fingerprint [3].....	4
Figure 1.2 : Hand Geometry [4].	4
Figure 1.3: Face Recognition [5].....	5
Figure 1.4: Iris Recognition [6].	5
Figure 3.1: Convolutional Neural Network [70]	53
Figure 3.2: Max Pooling [74]	55
Figure 3.3: Average Pooling [75].....	56
Figure 3.4: Sigmoid Activation Function [72]	57
Figure 3.5: Proposed Method [72].....	58
Figure 4.1: CNN Based DT Results With MMU IRIS Dataset	59
Figure 4.2: CNN Based RF Results With MMU IRIS Dataset.	60
Figure 4.3: CNN Based ANN Results With MMU IRIS Dataset	61
Figure 4.4: CNN Based MLP With MMU IRIS Dataset.....	62
Figure 4.5: CNN Based DT Results With CASIA-IRIS Dataset	63
Figure 4.6: CNN Based RF Results With CASIA-IRIS Dataset.....	64
Figure 4.7: CNN Based ANN Results With CASIA-IRIS Dataset	64
Figure 4.8: CNN Based MLP With CASIA-IRIS Dataset	65

ABBREVIATIONS

SVM	:	Support vector machine
NN	:	Neural Network
RBF	:	Radial Basis Function
ANN	:	Artificial-Neural-Network



1. INTRODUCTION

Session authentication is the control that is relevant everywhere that provides confidentiality used in building entrances and any system login or data transmission. Fragile stamping for authentication processes is used for purposes such as summary and secret sharing. Using a password to create security systems with biometric data is a work that hides and stamps the password used with encryption encryptions. Technological developments have made people's identity information compulsory. The purposes of the users who are allowed to capture other persons and components of this data by the law on the protection of personal data are targeted. It is very important to provide the necessary protection during the storage of personal data and the transportation of this information. Hiding data is very old. It was tried to be hidden in 1900 BC. In our recent history, the Vernam code was found by Joseph Mauborgne and Gilbert Vernam to be used in the First World War in 1917. In 1918, the ADFGVX encryption used in radio communication was found. In 1929, the Hill cipher based on linear algebra was introduced. In the 1940-1944 World War II, data hiding devices were found: Germans ENIGMA, British TYPEX, Americans SIGABA, Japanese RED&PURPLE. In 1970, the Demon and Lucifer data encryption was the basis of the currently used DES encryption. 1977 Ronald Rivest, Adi Shamir, and Leonard Adleman, RSA detainee. Respectively, ROT13 was found in 1980, ECC in 1985, IDEA in 1990, SHA-1 in 1995 and AES in 2000 [1].

Although digitization is used in many contexts, the core business asset is digital data, leading to changes in knowledge, wisdom, intelligence, action and business models. Digitization is the conversion of a physical item from analog to digital or digital representation for the purpose of digitizing processes, workflows. Digitization; It is the conversion of digital data, such as paper documents, microfilm images, photographs, sounds and video, into digital formats such as bits and bytes. Digitization, which occurs with the use of digital technologies, is the use of new values, opportunities and opportunities for gaining. The concept of digitalization is the process of digitizing information and making it available on various platforms, and the use of digital technologies for opportunities that can generate profit and value. Digitization is the process of activating, improving or transforming the business process with digitalized data sources and digital technologies, and the effective use and development of big data is a part of digitalization. The development of digital

technologies has taken a central position by making a significant contribution to the surveillance activities of governments, institutions and companies (Ünver, 2018). Today, advances in Internet spyware, video data analytics, artificial intelligence enable unprecedented detailed and analytical surveillance. While digital technologies make daily life easier, they also provide data to institutions, companies and states in order to ensure the continuity of their hegemony, without leaving an alternative escape point for the individual, especially the targeted individuals and groups. While digital-based tracking and surveillance technologies collect data on the daily life of the individual in the micro sense, they also provide surveillance in many different areas, including the economy, industry and entertainment sector at the macro level. Digital technologies provide worldwide surveillance opportunities by reducing surveillance costs, and the expensive and cumbersome systems of the cold war have been replaced by applications that use digital surveillance technology, from real-time facial recognition systems to smart cities. With the securitization process brought to the fore by the September 11 attacks, digital surveillance technologies have both become official and have been used extensively by the authorities. With digital surveillance, the surveillance and surveillance area gains invisibility, and it is not controlled where, for what purpose and through which mechanisms the data obtained from each movement of the individual is used. Digital technology-based devices are the most effective tools of surveillance mechanisms, and the data that emerges with the use of digital technologies also serves both authorities, institutions and companies to profile individuals and develop policies according to this profiling. Studies carried out under the supervision of states to protect their citizens against risks and threats have made all individuals a potential threat and as a result, the target of surveillance technologies [2]. The advancement and development of technology contributes to the development of surveillance and tracking systems, and brings with it a follow-up surveillance process, including cities, rural areas, agriculture, climate change, traffic, weather events, human smuggling and immigrants. Applications and programs such as Facebook, Twitter, Youtube, which serve on a global basis, also function as global surveillance mechanisms. Such programs and applications serving on a global basis are part of global surveillance systems. Cambridge Analytica's use of Facebook user data to influence voter preferences in the USA, Trinidad and Tobago is an important example of this. It has been seen that Cambridge Analytica is effective enough to affect the election

results by categorizing the individual from Facebook data and by exposing them to content that will change their preferences on a personal basis. Digital technologies contribute to the surveillance mechanisms of authorities and companies as well as the convenience and comfort they bring to daily life. As a result of the use of digital technologies, data are created, and they function as a source of information about the identity of the individual to surveillance mechanisms as footprints on movements, preferences and tendencies. Orwell's big brother character has become an integral part of the individual through digital devices, especially mobile phones. Companies and groups that benefit from authority and data, thanks to the opportunities brought by digitalization, from birth to death, whether in the private or public space of the individual; They archive all transactions as data, from selected friends to work, shopping and hobbies. With the services such as e-government and digital health introduced in this context, the individual has started to go online much more, and a surveillance process that goes to the center of the house and the most private personal area has started, especially with the use of health services for follow-up purposes. Based on this, digital surveillance technologies and application methods will be explained in this section.

1.1 FINGERPRINT RECOGNITION

Fingerprint is a type of biometric data used to distinguish people because it is different for every person. After the fingerprint data is obtained with the fingerprint device and sensors, it is recorded in the database. Fingerprint data recorded in the database is ready to be used in processes such as personnel tracking. Now, the personnel fingerprints are scanned and checked with the database registered in the system, and their entry and exit times are recorded. Figure 1.1 shows the block diagram of the formation of a biometric system. In the block diagram, firstly, biometric data is taken with the sensor, then after biometric data storage, the biometric data of the person coming for identity test and the biometric data in the memory are checked, the biometric data comparison is made, and the person identification process is completed [3].



Figure 1.1: Fingerprint [3].

1.2 HAND GEOMETRY

Since the geometric structure of the hand differs between individuals, it is used as biometric data. The geometric physical structure of the hand is used for authentication instead of identification. In hand geometry recognition systems, it is based on the principle that the hand placed in the hand recognition system is measured in three dimensions and recorded in the system. Recognition by hand geometry is not uniquely like fingerprints. Hand geometry is more suitable for person verification than person recognition. The measurement is made by considering the features such as length, thickness and curvature of the hand placed in the hand geometry recognition system. With the hand geometry recognition device shown in Figure 1.2, the structural feature of the hand is obtained with the sensor and biometric data is obtained [4].

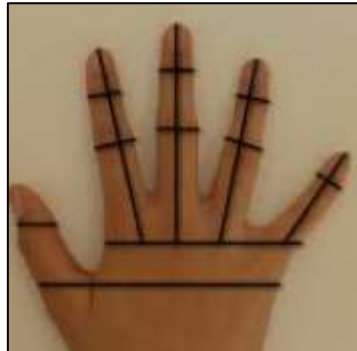


Figure 1.2: Hand Geometry [4].

1.3 FACE RECOGNITION

The face recognition system works according to the golden ratio principle. The pictures taken with the camera are recorded in the data system, taking into account the distances between the nose and forehead, eye and lips, nose and chin, as seen in the figure. Face

recognition systems have gained diversity according to moving image or fixed image, and today they are used in two systems. Figure 1.3 shows the structure of facial features used in face recognition systems. [5].

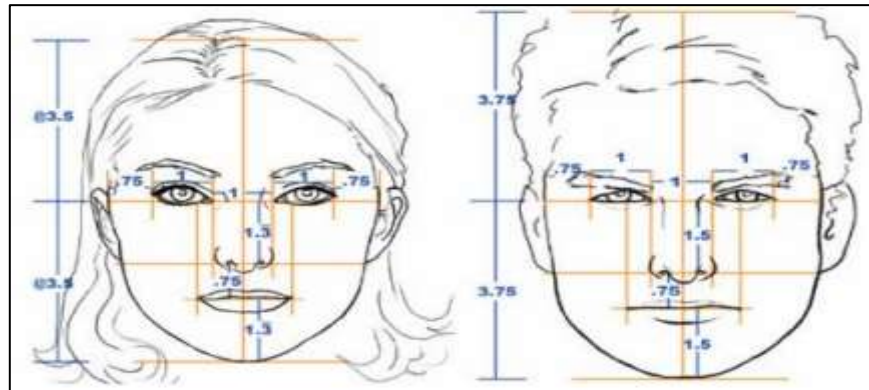


Figure 1.3: Face Recognition [5].

1.4 IRIS RECOGNITION

The iris in the eye is the colored part in the front of the eye, as can be seen in Figure 1.4. Since the colored part of the eye is the iris, it is photographed from a certain distance and used by converting iris information into digital data. Since the iris pattern is different in both eyes, the iris pattern should be taken for both eyes or the system should generate an algorithm according to which eye is taken. While the fingerprint biometric data consists of reference points, a rough value of 70, this is three times as much in iris recognition [6]. The process of iris image analysis involves extracting and analyzing various intricate features present within the iris structure. These features include the arrangement of crypts, furrows, and textures that form distinct patterns. The complexity and richness of these patterns make iris recognition systems highly robust against forgery and impersonation attempts.

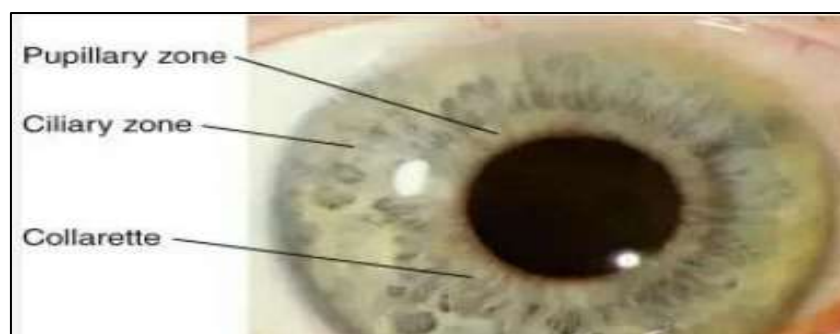


Figure 1.4: Iris Recognition [6].

At the heart of iris image analyzing lies the process of image segmentation, where the iris region is isolated from the rest of the eye image. This is typically achieved by detecting the boundaries of the iris using edge detection algorithms or circular Hough transforms. Once the iris region is extracted, various image enhancement techniques, such as contrast adjustment and noise reduction, can be applied to improve the quality and clarity of the iris image. Feature extraction is a critical step in iris image analyzing, which involves capturing the unique characteristics of the iris for subsequent recognition. One commonly used technique is to represent the iris as a two-dimensional texture pattern. The iris texture is typically described using techniques like Gabor filters, which capture the iris' intricate texture details at different orientations and scales.

The performance of an iris image analyzing system can be influenced by various factors. For instance, environmental conditions like lighting variations and occlusions can affect the quality of the iris image. To mitigate these challenges, preprocessing techniques such as normalization and image quality assessment are employed to standardize the iris images and filter out poor-quality samples. The efficacy of an iris image analyzing system is typically evaluated using benchmark databases that contain a diverse range of iris images captured from different individuals under various conditions. Performance metrics such as accuracy, speed, and robustness are assessed to determine the system's effectiveness and compare it with existing iris recognition methods. Overall, iris image analyzing plays a crucial role in biometric systems, offering a highly accurate and secure means of individual identification and verification. Through advanced techniques like image segmentation, feature extraction, and pattern recognition, iris image analyzing contributes to the development of reliable biometric systems with applications in security, access control, and forensics.

2. OVERVIEW

2.1 SURVEY

In the study of Venkatram, Reddy, Kishore and Shavya, using RSA-DWT, the patient's medical images such as MR were encoded and stamped. This way has been chosen to protect patient information. It has been stated that adding a stamp to medical images requires caution. 2 Patient's medical information is performed using RSA algorithm for image encryption and decryption. Medical images are stamped with the encoded patient image in the transform field using 2D Discrete Wavelet Transform. The main medical image and its imprinted image are converted into wavelet space and mixed. Finally, when these stamped medical images are transmitted over the internet together with the secret key to be used for decryption, the embedded encrypted watermark is extracted using 2DWT and the decryption key. The robustness of the proposed stamping techniques was tested with various attacks on stamped medical images, Peak-Signal-toNoise ratios and normalized cross-correlation coefficients were calculated to arrive at the quality of stamped medical images and extracted patient images. The results were generated for three types of medical images with one patient image stamping using four wavelets (haar, db, symlets, bior) at four different levels (1,2,3,4) using one keystroke. Experimental results have shown that RSA-DWT is superior to normal DWT [7].

Khamy, Korany, El-Sherif proposes an efficient stamping scheme based on sample comparison in the field of Discrete Wavelet Transform, where the cover sound is decomposed into several multiple subbands. The selected detail coefficients are replaced with a threshold value based on the embedding code image bit. This approach used an original image component to perform RSA encryption on it, then the encryption bits were embedded in the detail components of the audio signal according to a predetermined threshold value. The performance of the algorithm has been extensively estimated against attacks and simulation results are presented to prove the robustness of the proposed algorithm. Considering the experimental results, it has been tested to show a good PSNR and high data embedding capacity [8].

In the study of Nagpal, Bhushan, Mahajan, a study was conducted on digital image stamping developed for medical images using Neural Network, DWT and RSA. Three techniques for

image stamping namely; DWT, Neural Network (NN) and RSA encryption are used. As a result, the performance of the proposed technique was measured on the basis of PSNR, MSE, BCR, BER and NCC in the MATLAB R2010a environment [9].

Kumari and Yadav presented Biometric Steganography and non-biometric shorthand. The skin area and edge pixels were evaluated and the confidential data encrypted with the RSA algorithm was embedded in a certain area. Since the data is embedded in a specific region instead of the whole image, the security and quality of the stego image is increased [10].

In Garg, Gupta, and Khatri's study of fingerprint stamping and steganography for ATM transaction using LSB-RSA and 3-DWT algorithm, a combination of stamping technology and fingerprint authentication methods is proposed to provide copyright protection and authentication of digital images. Combined DWT with RSA and LSB while suggesting technique for better accuracy. In this study; Mismatch rate, false acceptance rate, mean square error, 3 accuracy and peak signal-to-noise ratio were examined and high values were obtained in DWT and RSA applications [11].

Bhargava presented new strategies in Mukhija's shorthand study of hiding image and text using LSB, DWT and RSA, where cryptography and Steganography mix information and additionally include insights from another medium through image processing. The encrypted picture is hidden in another image through the use of DWT strategies of LSB bits. It has been implemented using the set of cryptography and Steganography arrangements preferred in the MATLAB platform. PSNR and MKE were calculated, as well as the entropy of the cover image and stego image [12].

Kadhim Bermani's work, on the other hand, proposed a high-security model to hide the hidden image on the cover image of another image in which more than one algorithm is used, in the high-security Steganography model study based on DWT, DCT and RSA. The discrete wavelet transform algorithm and the DCT algorithm applied are to compress the hidden image and provide more space for the hidden image to be hidden, and the RSA algorithm has been applied to the encryption, making it more secure. DWT and RSA with CR used in certain quality measures such as PSNR and MSE to calculate the quality of this model [13].

Most of the existing methods in Divya's work on creating hybrid digital image stamping for Copyright Protection using DWT-SVD and RSA encryption focus on robustness and embedding capability, overlook security. This article introduced a new digital image stamping model based on hashing algorithm DWT and RSA asymmetric encryption algorithm to guarantee the security of confidential data on the basis of large embedding capacity, good robustness and high computational efficiency. In his experiments; It involves applying encryption algorithms of RSA to the stamping image and performing hybrid decomposition of Discrete Wavelet Transform and Singular Value Decomposition on the host image, and the stamping is embedded in the low frequency subband [14].

Kishore, Venkatram, Sarvya, Reddy In the study of creating medical image stamping using RSA encryption in the Wavelet domain, encryption-based medical image stamping of three types of medical images, MRI, CT and ultrasound, is used. The stamp used in this application is the patient image. The stamp patient image is encrypted using a public key encryption with the RSA algorithm. The cover image is a standard resolution medical image to be stamped. The RSA encrypted patient image is placed on the medical cover image in the wavelet transform area. The inverse wavelet transform is applied to create a stamped medical image with the patient image as the stamp. The stamped image was tested both in visual quality and quantitatively using PSNR and normalized cross-correlation [15].

Solanki, Malik, Chhikara's proposed study of RONI (Region of Non Interest) medical Image stamping using DWT and RSA is about storing patient information in the medical image itself, which can be a CT scan or MRI image. First, it is divided into two main stages to determine the ROI (Region of Interest) and RONI of the image. Here, ROI is defined as the informational portion of the medical image and RONI is defined as the non-informational portion of the MRI image. It will prevent the user from destroying valuable information from the view. The stamping is encrypted using RSA. The second stage is about hiding the image to RONI. A DWT-based approach is used to hide such information. General Conditions are to provide two-way security to medical images using DWT and RSA, along with the protection of ROI [16].

For authentication of biometric images, stamping was done using encryption techniques. Biometric data was used for authentication; For high security, biometric data and a password were used, the weakest point of the system was encrypted with RSA encryption, and then

the biometric data was stamped with DWT and security measures were taken. In the second part of this study, biometric data is introduced. Physiological data, which are divided into physiological and behavioral, are defined as fingerprint recognition, finger vein print, hand geometry, face recognition, eye recognition and DNA recognition. As behavioral biometric data, voice, speaking style, keystroke rate and signature were taken into consideration. In the third chapter, information about stamping and stamping types is given. In stamping, especially the digital stamping LSB, DWT, DCT, DFT SVD stamping methods have been examined and DWT, which is the subject of the thesis, has been discussed in detail. Information about stamping error rates, signal to noise rate, normalization, bit error rate is given. Information about attacks such as noise addition, clipping, JPEG lossy compression, re-stamping, geometric attacks, and scaling, which is another subject, attacks on digital stamping are given. In the fourth chapter, information about encryption is given. In particular, information about symmetric keying, block cipher, public key cryptography, encryption protocols are given as encryption types. RSA encryption is explained in detail and information is given about side channel attacks and crypto analysis attacks, which are types of attacks on RSA encryption. In the fifth part, fingerprint data encryption with RSA, steganography with LSB method and stamping with DWT are done. MATLAB results and outputs are given. In the sixth chapter, the findings obtained in the materials and methods part are given and the importance of the subject is explained.

2.1.1 Denial of Service Attacks (DoS) Message

While the political struggle that started with controlling the land was carried out over the means of production in the modern age, where factories and machines became important, today, with the importance of data, a political struggle is being made to control the data flow. At the point where digital technologies come from the internet infrastructure, surveillance has become global rather than national. Thanks to the digital technology infrastructure, the individual is subject to both national and international surveillance. As a result of this, the individual, who is monitored and followed by the authority, can be followed not only within its own national borders but also in the international arena. In recent years, it is seen that states have allocated resources especially to digital surveillance applications. International follow-up and surveillance can also be carried out for the targeted individual, group,

institution, company. Countries with developed economic level and technologies keep other nations under surveillance and follow-up at the rates they bear the costs. Therefore, they oversee the acquisition and processing of data belonging to other nations. In this context, it is aimed to obtain all kinds of data from industrial production to public finance, from social morale and dynamics to military preparation, in surveillance and follow-up processes. In the context of state versus state, state versus society, states try to get strategic information from each other while trying to avoid surveillance processes of their own information. One of the first known applications in the field of surveillance is Promis (Prosecutor's Management Information System) and its derivatives, which emerged in the 90s. The program infiltrating the target system is to be able to reveal similarities and differences through the sample by automatically performing search, scanning, information gathering, monitoring and finding. One of the emerging applications of international surveillance is Echelon, which is an important part of the vast intelligence network established to decipher, control and listen to all kinds of communications around the world. It is one of the most important mechanisms of the surveillance network, which was established in 1971 with the code name ECHELON, in Australia, Canada, New Zealand, England and the USA, whose roots go back to the UKUSA agreement in 1941 and known as the five eyes. It monitors all kinds of communication and enables its storage. For this purpose, data is obtained by satellite signals, microwave signals and also by listening to cables crossing the ocean. Although the existence of such institutions that carry out surveillance and follow-up on a global scale is not accepted, it has been revealed that the US National Aeronautics and Space Administration is observing and following both nationally and globally, with the disclosure of NASA employee Edward Snowden in June 2013. The Carnivore system, which was used by the FBI in the 2000s to monitor written communication, was used to control millions of correspondence over the internet and to obtain systematic data. Thanks to the mobile tracking programs known as Dreamy Smurf, Nosey Smurf, Tracker Smurf, Smurfs (Smurf Suite) for mobile tracking purposes by the American National Aeronautics and Space Administration (NASA) and the British Government Communications Headquarters (GCHQ), surveillance can be performed even if the individual turns off his phone. Snowden, 2013). Today, many different programs and applications are used, especially by the authorities, for the purpose of monitoring and monitoring the individual. Software and applications such as deep pocket inspection and mass digital surveillance platforms such as Remote Control Systems, Phorm,

PackageShaper, Hacking Team, FinFisher and Procera Networks are some of them (Ünver, 2018). Today, authorities provide surveillance technologies through private companies and institutions instead of developing themselves. Many different systems, including satellite and aerial surveillance technologies, are used in the surveillance and control of borders. Cameras and satellites equipped with sensors are used to monitor the movement of immigrants, the capacity and mobility of refugee camps, the movement of large objects such as boats and the detection of border violations. Satellite images have been used for a long time for the surveillance and tracking of immigrants. Frontex published satellite images in 2015 where it detected 370 migrants in inflatable boats off the Libyan coast. The European Border and Coast Guard Agency, Frontex, uses unmanned aerial vehicles to detect ships and boats of migrants trying to cross into Europe. Among the drones that the European Union has deployed to the Mediterranean after the end of Operation Sofia are Hermes, made by Elbit Systems, and Heron, manufactured by Israel Aerospace Industries. Data from these systems are also shared with third countries. For example, Frontex provides such information to the Libyan Coast Guard.

2.1.2 Crime Control and Administrative

Surveillance of the State Especially after the September 11 attacks, groups such as minorities, different religions, sects and immigrants began to be seen as threat factors in the general population, and digital-based surveillance and follow-up implementation mechanisms began to be widely used. In particular, resources are allocated for surveillance and tracking systems within the scope of preventing crime, including European Union Member States in different parts of the world and in democracies, which stand out especially in the Chinese state. Especially by the European Union, large resources are allocated through Frontex for current digital technologies for the surveillance and tracking of immigrants. Digital devices also act as surveillance tools. Digital footprints are created at every stage, from shopping to the hospital visited, to the holiday, and these traces are transferred to data pools and archived. This also reveals that data is the most important part of surveillance mechanisms. Surveillance mechanisms also have an impact on the individual's attitude, behavior and actions. The behavior of the individual, who is under constant surveillance, also becomes stereotyped in the process. Although security camera systems and similar

technologies have some benefits, they have an impact on the individual's attitudes and behaviors, whether in traffic or in his daily life. Surveillance mechanisms do not only categorize the data they obtain from the individual, but also resort to ways to influence the attitudes and behaviors of the individual in order to obtain results when appropriate.

2.1.3 Control and Surveillance of Working Life

Digital technologies have also brought about great changes in the working environment, with applications such as flexible working and working from home, Bentham's metaphor of the physical panopticon has been moved far beyond, and thanks to GPS and other internet-based systems, the work flow of the individual is followed even if they are not in the same environment. Institutions, companies, governments follow their employees and keep them under surveillance by various methods from the moment they enter the workplace. While the individual, who is under surveillance at the job application stage, is determined from his/her social media accounts and with whom he/she is in contact, disease and other registry information can be obtained from different applications. Surveillance processes develop with digital technologies and find their place in all areas of life. In this context, disciplinary surveillance has ceased to be a single center and has become inclusive of all individuals³¹ including schools, hospitals, prisons and especially factories and workplaces. More efficiency, surveillance for profit has not lost its function, on the contrary, it continues to increase and expand. At the point where digital technologies have come, the surveillance of working life is not limited to the workplace. Thanks to digital data, companies have the opportunity to observe the past as well as the present state of the individual. From the data on digital media environments, it is possible to look at the history of the individual to be employed, to find it, and to follow the individual he employs through these channels. In the business environment, even the key pressed by the individual on the keyboard is recorded through computer tracking programs, working hours are tracked by pressing fingerprints and cards. are kept under surveillance. Therefore, digital-based surveillance mechanisms also have a disciplinary character in business life.

2.1.4 Consumption and Consumer Surveillance

With the development of technologies and the use of computer systems, consumer profiles have begun to be created, and a process in which consumption habits are included in the

surveillance process has begun. With the development and spread of technology, the mechanisms for consumption and consumer surveillance have also developed. While companies are keeping the consumer under surveillance and archiving all kinds of data about their daily life, on the other hand, they have started to use artificial intelligence technologies in their infrastructure for the analysis of this data. It is seen that these companies benefiting from the data use the most up-to-date digital technologies. The most up-to-date technologies that collect data on the health of the individual through fingerprints, face recognition, iris and smart watches and wristbands were brought to the fore by these institutions and companies, which also benefit from the data. The fact that digital surveillance systems surround the individual and generate data from his/her every move brings with it the tracking of the individual for marketing purposes and exposure to personalized marketing and similar instruments. With digital marketing and advertising applications, individuals are exposed to advertisements and similar applications without the concept of time and place. With the synthesis of digital surveillance applications with artificial intelligence applications, advertisements have become personalized on the basis of the individual's needs and needs. Personalized marketing applications, blogs, news sites, and search engines associated with the individual's social media and derivative application profiles are the biggest sources of income. The demographic information provided by the individual, the IP address of the digital device used, the application's IP address, the logs of past behaviors, searches, reviews, and the records of the shopping transactions are obtained by digital-based surveillance mechanisms and evaluated in marketing and similar areas. Monitoring is carried out to obtain data such as the taste of the individual, friend groups and interlocutors, purchasing power and frequency, and the correct target orientation of the advertisement is ensured by making calculations about the product to be purchased and the advertisement to be clicked. These data collected about the user and consumers are mostly obtained from IP-based digital technologies, language, geographical location, pages viewed, time spent, advertisements seen, texts read, videos watched, music listened, products viewed and all kinds of shopping activities are recorded as data data, It is used when necessary or marketed to other companies and institutions. Institutions, companies, for marketing purposes, to obtain the information of consumers and users and present it to use in a systematically classified way when appropriate. In this context, artificial intelligence-based systems are profiled by making a

meaning out of every move made by consumers and users during their use of digital media, stored as data, and sold when necessary.

With NFC (Near Field Communication) Near Field Communication technology, which is one of the most up-to-date technologies used in acquiring consumer data, information about where, when and what an individual has received can be obtained. It is known that Google, in particular, allocates resources to this technology. Companies such as Facebook, Google, Twitter, digital media platforms such as navigation, e-commerce, entertainment, social activation, while making the life of the individual easier and comfortable, on the other hand, have come to dominate the data that will make the individual get to know him better. As a result of this, it is digitized and coded in the individual and becomes usable in all kinds of data mining, especially in marketing activities. The classical panopticon, which watches over the body of the individual, becomes invisible, leaving its place to the invisible eye, the eyes. Individuals are heavily exposed to surveillance mechanisms for marketing and advertising efforts to increase consumption. As a result of this, surveillance is not only limited to certain limits, but continues to expand its impact on the whole society. Production and all kinds of needs of the individual, especially consumption, have gained a global cosmopolitan character. Therefore, the individual creates data on a global basis while meeting his daily needs. 33 The digital advertising industry, which is controlled by the world's largest companies, is experiencing major disruptions in the implementation of basic standards such as human dignity, freedom and respect for private life. This is also due to the fact that the digital advertising industry is more controlled and used for marketing purposes by computer and technology companies rather than media and content providers. The individual does not have a control mechanism about how private information about himself results, which data is collected by whom and interpreted by whom. Individuals can be exposed to very different panoptic surveillance processes in their daily life, banks can profile their customers and give them priority in incoming phone calls. Commercial organizations that benefit from data have a huge economic power, and these companies, especially those working on a global basis, have the power to influence the political power and authorities in any country, especially in their own countries. One of the most obvious examples is the use of individual data as a marketing element for advertising and political purposes in the Facebook Cambridge Analytica scandal. Therefore, legal sanctions for the protection of personal data and e-commerce regulations should be supported by clear and strict rules.

2.1.5 Digital Tracking

Surveillance Technologies Digital technologies contribute to the surveillance mechanisms of authorities and companies as well as the convenience and comfort they bring to daily life. As a result of the use of digital technologies, data are created and they function as a source of information about the identity of the individual to surveillance mechanisms as footprints on movements, preferences and tendencies. Orwell's big brother character has become an integral part of the individual through digital devices, especially mobile phones. Companies and groups that benefit from authority and data, thanks to the opportunities brought by digitalization, from birth to death, whether in the private or public space of the individual; They archive all transactions as data, from selected friends to work, shopping and hobbies. With the services such as e-government and digital health introduced in this context, the individual has started to go online much more, and a surveillance process that goes to the center of the house and the most private personal area has started, especially with the use of health services for follow-up purposes. On the one hand, human life is facilitated, on the other hand, applications, location information, use of social media, which are used on devices with digital technology infrastructure, consciously or unconsciously contribute to monitoring and surveillance tools. At the point where digital technologies have come, data has become very valuable and the individual is represented as numbers and codes by digitizing. Free digital media applications used by the individual may have turned him into a product of the application rather than a customer, if digital-based programs and applications are used free of charge, it means that the individual has become a product. The classical panopticon, which is made by disciplining and punishing physical bodies in physical space, has developed and changed thanks to the opportunities and possibilities brought by digital technologies, and has come to a position to establish hegemony over the attitudes and behaviors of the individual without the need for physical space and physical body. The data generated as a result of the use of digital technologies has ceased to be an ethical problem and has begun to find a place for itself as a political and economic problem. It assists the authorities in private companies in the development, use and operation of digital-based information technologies, which provide convenience to authoritarian regimes in the surveillance and monitoring processes of individuals. In this context, he worked with social media companies while creating the Orwellian travel and social credit system of the

Chinese state. Digital surveillance tracking capability depends on the technological infrastructure and capacity of the authorities. Both the perspective of surveillance mechanisms and the way they are implemented will be different between authoritarian and totalitarian and authoritarian countries, China, Pakistan or Singapore, which are governed by liberalism that incorporates technology. It involves using advanced techniques to perform an audit, such as digital tracking, surveillance, but also data mining or software robots. Big technology companies such as Microsoft, Amazon, Google, Netflix, Apple, Facebook, called Big Tech, serve millions of users and therefore they can have a say over user behavior as well as control of user data. The practices of these companies regarding the privacy of the individual still do not inspire confidence despite all legal sanctions, and it is very difficult to enter this ecosystem from outside, and it is estimated that it may not be possible to live in the digital world without their support [17].

2.1.6 Industry 4.0 and Smart, Integrated Systems

Industry 4.0 is the creation of new applications on a completely individual basis, in which the virtual and physical manufacturing system are integrated with each other, creating the fourth industrial revolution by making smart factories possible. In addition to these, it is the simultaneous work of synthesizing renewable technologies from nano technologies to quantum computing, from gene sequencing. The fourth industrial revolution enables the interaction of biological, physical and digital fields [18]. With Industry 4.0, factories with networked, sensor-equipped and smart machines are created, on the other hand, Industry 4.0 compatible devices and machines are produced from these factories. Therefore, devices interacting with each other also create an ecosystem including big data. As a result, the combination of artificial intelligence techniques, data and scalable infrastructure changes the way of life and management of society by affecting various factors including business model and socialization. These processes are also effective in surveillance and follow-up mechanisms, enabling the process to be carried out with more data and less cost and effort. With Industry 4.0, the systems and devices used by the individual communicate with each other via Bluetooth, Wifi and similar communication protocols and data is shared in real time. The control of mobile phones, televisions, air conditioners, ovens, refrigerators, toothbrushes and lamps, and the integrated operation of phones and computers can be evaluated within this scope. Intelligent devices and automations not only make life easier for

the individual, but also create very fast and large data stacks. The data obtained from all these automation systems disclose the individual by providing data in the surveillance and control mechanisms of authorities, institutions and companies at the same time.

2.1.7 Web 2.0 and Cloud Computing

With the foundation of Web 2.0 and Cloud Computing Digital media applications on Web 2.0, everyone has become able to watch everyone, and the individual who receives information can also give information, produce information, share information and receive feedback on the results. A mutual interaction occurs as a result of the environments where applications such as Youtube, Wikipedia, Twitter and Facebook work, where the individual is actively involved, and as a result of producing content and consuming the content, therefore, digital media applications can provide data flow to the surveillance and tracking systems of the individual. With Web2.0, the potential for data capture and processing has been provided to surveillance mechanisms by enabling the production of digital data on an unprecedented scale and at unattainable speeds. Cloud computing is a technology that offers low cost, high speed and high amount of redundancy, and enables fast connection of all devices and applications using internet technology, from anywhere, anytime. While it offers data centers advantageous in terms of hardware, software, energy and security to institutions and companies, it also gives individuals the opportunity to access data in the fastest way. There are institutions providing cloud computing services such as Amazon (AWS), Google (Cloud Platform), Microsoft (Azure), IBM (SoftLayer, Bluemix). In all these processes, cloud computing provides great opportunities to authorities and other institutions for surveillance and follow-up purposes. Weather and satellite systems used for surveillance and tracking purposes can also use cloud computing for the calculation task. They can transfer the data they obtain to cloud services such as Amazon AWS without the need to mount satellites on super-powered computers. Thanks to this, more transactions, more information and a scalable structure are offered, while on the other hand, these satellites are used for longer periods because they are not limited by technologies.

2.1.8 Big Data Analytics and Information

Obtaining data from all kinds of devices and processes such as sensors, social media usage, video-audio operations, GPS signals, phones is called Big Data Analytics. (According to IBM) It is the making meaningful of data obtained from all kinds of social media sources such as statistics of Internet-based digital devices and systems, phone call records, blogs and videos. Big data has three basic elements that distinguish it from traditional data: variety of data, volume of data, and quick access to results. The volume of big data is large and contains information and data from many unstructured sources such as audio, video, text, maps in mixed formats. With Industry 4.0, the continuous production of data by machines, the mobility and mobility brought by internet technologies is a very important factor in the individual's access to data from anywhere at any time, and at the same time increasing the size of the data. The data produced today has reached enormous dimensions. The content of this data includes all kinds of information, including security, defense, marketing, banking, health, economy and contact information. Both governments and institutions and companies have huge data stacks and structures. These data, which are generally obtained from internet-based digital devices and systems, contain pictures, audio, video, location and many other data belonging to the individual. While the states highlight the security threat, other institutions and organizations subject this data to monitoring and surveillance mechanisms for marketing purposes. The power exerted by the authorities over the lands and armies in the historical process has left its place to the data today. The huge size of the data and the continuous formation of data in addition to the existing data has led to the emergence of deep learning systems, pushing the surveillance, supervisory authorities and companies to new searches. 37 The reason big data is so important is that it is about making sense of unstructured data using it. Considering that most of the data in the world is unstructured and raw data, great opportunities arise for businesses if the difficulties in obtaining, storing, researching, sharing, analyzing and visualizing such voluminous and unusable data are overcome. Data analytics allows to consolidate silos of collected data. Data analysis and data storage are not enough, they also need to relate data to process analysis and bridge the gaps between machine learning and data mining. The common point of applications such as analysis of hospital treatment processes, understanding the browsing behavior of customers shopping on the website, analysis of materials passing through x-rays and baggage handling systems is that dynamic behavior is related to process models. The extensive collection and

further processing of personal information in the context of Big Data analytics has raised serious privacy concerns, particularly in relation to large-scale electronic surveillance, profiling and disclosure of private data. To allow the full benefits of analytics without invading the privacy of individuals, it is extremely important to draw the boundaries of big data processing and integrate appropriate data protection measures to the core of the analytics value chain.

2.1.9 Combining the Eye with Artificial Intelligence and Biometric

Mass Tracking One of the most important resources that individuals use to communicate with each other is voice. Voice, which has a very rich environment in terms of human communication, also tells a lot in terms of intonation. In this respect, audio technologies are used in digital technology infrastructures, especially smart home systems, smart assistants, smart phones, televisions, multimedia devices, in order to make the life of the individual comfortable. Therefore, voice-controlled devices and technologies are used extensively by the individual. Voice recognition, voice analysis systems and applications are used extensively by financial institutions. Worldwide, 31% of smartphone users used voice technology at least 52 times in 2019, while 20% of Google-based systems were with voice search. Audio signal analysis can provide the diagnosis, classification of the individual, the determination of the group to which he belongs, as well as the remote surveillance and follow-up of the individual. Factors such as diseases and headaches affect the vocal cords and change the voice of the person. In the next stage, it is aimed to diagnose the diseases of the individual. Voice analyzes using artificial intelligence can also be used in surveillance and tracking systems to determine the mood of the individual. Therefore, each individual's unique, rich-featured voice creates a great potential for surveillance and tracking systems. These systems are also used for the surveillance and tracking of immigrants. In this context, speech recognition, analysis and programs are used by using linguistics in order to verify the origin claims of immigrants. In the European Union, there are also studies on the right of everyone to exist in public spaces in a free and dignified way. The European Parliament has banned the sale of digital surveillance systems in a way that harms human rights, democracy and freedom⁴¹ in 2011, although some member states and institutions are carrying out legal studies that will encourage and enable biometric mass surveillance. Although countries such

as Portugal, Italy and Serbia have put them on the shelf for now, they have been in legal studies that will encourage and enable biometric mass surveillance. Biometric surveillance systems enable authorities, institutions and companies to fully automatically monitor public spaces at all hours of the day. Facial recognition and artificial intelligence are seen as the biggest threat facing society. These systems, which are heavily used in countries without democracy concerns, are also used in public spaces throughout the EU by emphasizing the safety factor. The rights and privacy of the individual are violated on a mass basis. Such systems can also deter the exercise of the individual's most fundamental right, the right to demonstrate and march. These systems, together with criminals, subject the whole society to surveillance processes as a target and form the infrastructure of mass surveillance. Artificial intelligence-assisted surveillance technologies may not always give accurate results and may cause errors that can cost human life. The story of the Palestinian worker, who was arrested by the fully equipped Israeli state law enforcement officers as a terrorist, as a result of the text "good morning" in Arabic being perceived as an "attack" by Facebook algorithms. It is an important example showing that it can be shown (Harari, 2018: 74). The advantages of digital surveillance technologies to authoritarian regimes can emerge in many different places. In the example of the Chinese state, social media, in addition to intrusive surveillance on digital channels, follows the body of the individual everywhere with the face recognition system within the scope of the Skynet Video surveillance project, which is constantly followed. Listening to certain sounds from anywhere with automatic detection systems, computer and mobile phone data are collected from Wifi sensors and the correspondence of the individual is also followed. Data silos created by collecting all kinds of data and information, including license plate tracking systems, banking and health data, are subjected to artificial intelligence algorithms and risk and threatening behaviors are sought. This data mining and social credit system serves to become a totalitarian state as a result of digital surveillance, supervision, and there is no obstacle to totalitarianism (Boo, 2021: 25). All these practices facilitate the tracking of Xinjiang Uyghur and other minorities, unwanted groups and immigrants, which are categorized within the framework of banoptic surveillance. Biometric data can also be used to create secret watch lists, files and profiles. The European Union uses biometric technologies for identity verification purposes. Automatic fingerprint recognition technology is used by SIS II, Eurodac, VIS systems.

Studies are underway for the use of automatic face recognition systems (FRT) in the near future [20].

2.1.10 New Payment Systems and Social Rating

Discrimination refers to unfair or unequal treatment of members of a category or minority, regardless of individual merit. Credit scoring systems, which are automatic decision systems used especially in the field of banking, are used very effectively thanks to the ease of data collection. At the same time, individuals are classified by data mining from data sets collected by including historical data (Ruggieri, 2010). Therefore, by means of data mining, the individual can be classified by automatic systems and exposed to discrimination. With digital-based surveillance mechanisms, the individual has become an object that is subjected to various processes, processed, classified, evaluated and marketed (Öztürk, 2013: 138). While the surveillance mechanisms focus on the control of the individual by emphasizing the safety factor, on the other hand, the economic interests are brought to the forefront in the surveillance carried out by institutions and companies, and especially artificial intelligence supported marketing strategies based on increasing consumption appear as the area where surveillance applications are most intense. Various applications are being developed for the dissemination by governments and especially companies and businesses. It is a system that reveals the economic orientation of the individual and reveals results accordingly. This system, which was first implemented by the Chinese state, is being implemented in different countries in the world, and the Chinese State is one of the best examples in this regard [21]. In this regard, although direct applications are not seen in the European Union, it confronts the individual in a very different way. For example, in Germany, the credit rating agency "Schufa" functions in many different areas, not only with the withdrawal process. Even for the rental house, Schufa data is available to the individual. In this system, where millions of people have data, all kinds of financial status of the individual are followed. Therefore, the social scoring system, which has come to the forefront by the Chinese State, has very different reflections in the most democratic countries of the world. There are many different surveillance and tracking practices in the social scoring system. While the authorities and private institutions access all kinds of data of the individual, the individual also bears the necessary responsibility, and the applications and programs he uses have the opportunity to

score every institution and individual with which he is in contact with beekeeping. For example, with applications such as post-shopping service quality and evaluation score of the courier, everyone has the opportunity to rate everyone and see the scoring status. Here are the most obvious examples of omniscient surveillance applications. It is seen that some unethical, inhumane, surveillance and follow-up mechanisms implemented by China and other states are applied with different methods in Europe and other western states. For example, it is seen that the social scoring system, the simplest example of which is implemented by the Chinese state, is not in official transactions in Germany, but in transactions such as banking transactions, contracts and house keeping with "Schufa". While the surveillance mechanisms focus on the control of the individual by emphasizing security, on the other hand, the economic interests come to the fore in the surveillance made through institutions and companies, and artificial intelligence supported marketing strategies based on increasing consumption appear as the area where surveillance applications are most intense.

2.1.11 Digital State and Digitization of the Individual

Data generated by the use of digital devices are also footprints of the individual and provide clues to surveillance mechanisms about their preferences and identity. Today's society is in a digitalized state. The data stored in cloud servers are electronic files, so they are kept as electronic files on digital platforms, from the song the individual listens to the book they read, to their bank accounts. States obtain the information of the individual in order to fulfill their duties towards their citizens and continue to use these data by making additions to this data in all areas of the individual's life. With the emergence of digital technologies, states have started to implement e-government applications in order to provide faster and higher quality service to their citizens. With the electronic government, it is aimed to ensure that the individual reaches quality, fast and uninterrupted service in the shortest and easiest way, on the other hand, the individual is identified through an identity number given to him. In such systems and applications, the individual is digitized and represented by numbers and codes. This number is now integrated with the individual and has become a digitized personality with this number that the individual uses in all kinds of transactions. With services such as e-government and e-health introduced in this context, the individual has started to be online more both institutionally and individually. Especially with the Hayat Eve

Sıgar (HEPP) application, the use of digital-based applications has increased and a surveillance process that goes to the center of the houses has begun to be experienced. With the increase in digital-based applications, the surveillance and follow-up processes of authorities and companies have become easier, and surveillance has moved to different dimensions with the participation of surveillance mechanisms in cybercrime. Authorities, institutions, companies, who benefit from data for both security and profit purposes, have made the individual an instrument of digital technologies, digitized and represented by codes. Within the scope of the European Union digitalization studies, the free movement of goods is based on computerized public transportation, and applications such as security and Schengen information system are available in data systems as digital data [22].

2.1.12 Digital-Based Surveillance Methods of the Individual

There is no other device that produces data as much as the digital-based smart phones used by the individual. These small but ingenious devices are primarily used for basic communication, while on the other hand they are used as internet use and personal assistants. It also functions as an excellent tracking, surveillance tool. Thanks to the feature of hosting e-mail, text, SMS, social media applications, location information can be obtained with whom and how often the individual communicates, where the individual goes and with whom he/she communicates with the map application, GPS. Thanks to the web application, information about internet searches, information about friends and social environment with the guide feature, and information about hobbies and personal curiosities and tendencies can be obtained thanks to the applications used. Again, thanks to the applications used, information about the consumption process of the individual such as banking and shopping, smart wristband, watch integration and health and sports applications, the most basic health information and comprehensive data about the health and medical history of the individual, including heart rate, are constantly transmitted to the surveillance mechanisms and kept up to date.

Despite the important role digital technologies play in our daily lives, little is known about how they document our experiences and how the resulting data is collected, by whom, and ultimately used. The European Union and Member States allocate large budgets to surveillance mechanisms, information technology systems within the scope of controlling

immigration and effective control of external borders. Information technology systems for border surveillance, at border crossing points; It was established to control immigrants at land, ports and airports. Information technology systems are concerned with controls over people, objects, visas and asylum applications, fingerprint comparisons and passenger records. The authorities, who follow every step of the individual for surveillance and follow-up, have gained the opportunity to reach much further dimensions with machine learning and artificial intelligence. With sufficient data and information facilities, mechanisms that know the individual better than him or her have emerged. With these mechanisms, it has become very difficult for the individual to isolate himself from the intelligence structures of the surveillance authority and private institutions and organizations. From the use of the Internet to the use of social media, the individual is subjected to profiling in many aspects such as eye movements, pulse rate and information that should be confidential. These institutions and companies, which have data that even the individual does not know about himself, make high profits [23].

2.1.13 Individual's Interview Traffic Surveillance

Digital technologies contribute to surveillance mechanisms by producing data, consciously or unconsciously, in a way that is constantly ready for surveillance due to their infrastructure. It is known who the individual is, where he is, his location and with whom. Therefore, heaps of data on the identity of the individual, what he does, consumption and related issues flow to surveillance mechanisms. Edward Snowden, who revealed the worldwide eavesdropping of the US secret service with Wikileaks documents in 2013, remained on the agenda for a long time. States communication tracking is done through a legal institution for surveillance. In cases where legal eavesdropping is incomplete, monitoring and surveillance of target individuals, groups or states can be carried out by using technical and cyber intelligence systems, special programs, spyware and internet technologies. Verbal communication of the individual can be done by listening to the environment, over-the-air listening and spyware. In this context, especially speech recognition technologies come to the fore and individual speeches can be included in a meaningful text.

2.1.14 Movement of the Individual, Location Surveillance

The movements of the individual in daily life, including their routine movements, create very large digital traces. Systems and applications such as mobile phone networks, satellites and global positioning systems (GPS), detailed recording of telephone calls (CDR) assist surveillance mechanisms in networking and collecting the individual's movement. Based on these data, a high degree of predictability is provided about the individual's future positions by extracting quantitative patterns of the individual's movements [24]. The Global Positioning System (GPS) detects the precise location, movement speed and direction of the individual, and where the system is lacking, Bluetooth technology is activated and a point-based location is taken. It assists the surveillance mechanisms in acquiring the individual's location information, especially over GPS and GSM (Global System for Mobile Communications) networks, both in the direction of movement and in time.

2.1.15 Written Interview Surveillance of the Individual

For the purposes of surveillance and control, the states have established legal mechanisms to monitor the written communication of the individual, and spyware and applications are used where there are deficiencies. The ubiquitous surveillance process that has emerged with digital technologies also means surveillance against everyone everywhere and creates a situation where there are no borders. This situation also causes an increase in transparency and accountability concerns[25]. The fact that Facebook data, which emerged with the Cambridge Analytica scandal, can be used for political purposes, and that even the voting right of the individual can be manipulated by rendering it dysfunctional

2.1.16 Individual Tendency, Lifestyle Surveillance

An individual's life is a producer of facts that can be concealed and analysed; While the lifestyle of the individual is evidenced by the purchase records, the movements of the individual are explained from the GPS and mobile phone traces records. The digital technologies used by the individual leave digital traces, while these traces reveal who the individual is and their interests, on the other hand, they can predict what the next step may be. In recent years, the individual has become the main wheel of these technology companies thanks to the data he has provided to several technology companies, while on the other hand,

it provides low-cost surveillance in digital environments. While accessing all kinds of information about an individual such as health, finance, security, political views, it remains a separate mystery how much attention is paid to its legal dimension. Thanks to the applications and programs they develop, these companies constantly deprive the individual of themselves. Digital technologies are used for surveillance, data mining and data analytics also provide population controls. Especially with the introduction of big data, self-learning artificial intelligence and algorithms, the surveillance process evolves into different areas, and the process progresses automatically with little cost and little effort. Authorities, companies know the individual better than him. The prominent issue here is that the individual is exposed to various manipulations due to the prediction of the next step rather than surveillance. The conveniences brought by digital technologies, in addition to practical solutions, also sometimes threaten the human rights and freedoms of the individual by eliminating the boundaries between the public and private spheres. Data sharing over digital-based media applications not only affects the privacy and security of the individual, but also affects the institution, the social class, and sometimes the general society, causing effects such as exclusion, discrimination, disclosure and targeting. Daily movements of the individual, membership and use of social networks, activities such as phone calls and e-mail are some of the applications that leave digital traces. While using the digital technology infrastructure, the individual constantly provides data to technology companies and authorities. Thanks to the artificial intelligence algorithms of the programs and applications used, it comes before the person related to the interests of the individual. The individual is exposed to advertisements related to what he is most interested [26].

2.1.17 Digital Dictatorship

Authorities are working on digital surveillance mechanisms for tight controls over the individual, including online information, accompanied by intrusive surveillance to ensure political control. The most obvious example of this is the Chinese state, leading the world by combining surveillance, censorship and coercion for political stability, there are states that take it as an example, and their number is increasing every day. Powerful states and technology companies need to accept that they can use digital technologies in ways that restrict the freedom of the individual beyond the world to authoritarian, totalitarian regimes. Artificial intelligence-based digital surveillance can evolve into a world of digital

technologies where the freedom of all individuals is restricted and weak. This knowledge and power, which artificial intelligence and machine learning have reached and will be carried to higher levels in the future, also has the capacity to emerge as a Digital Dictatorship. Certain institutions and organizations that control the data will be in a position to decide in the next stage to establish practices and mechanisms for dominating the human body. This will also be a period when technologies for the development of body and mind will take place instead of industry and other manufacturing sectors [27]. Oversight, which is important for public safety, can only build trust in society within the scope of transparency and accountability. Otherwise, digital-based tracking on a global scale will ensure the continuation of surveillance institutions and companies in a process that benefits from all kinds of data of the individual, including biometric data. Digital surveillance mechanisms that are not transparent, accountable and not regulated according to ethical rules condemn authorities, companies, institutions and individuals to exploitation over their data. One of the biggest questions facing the individual is how to make sure that surveillance is only for the purpose of countering threats or criminal activities and not for the purpose of controlling or monitoring political opposition groups or non-governmental organizations. The answer to this question will help resolve the impasse between retrospective accountability and sensitive information, the gradual release of these secrets after their time-sensitive nature is over, and surveillance and privacy. The functional of democratic and legal ways, based on the rule of law and agreed upon, will remove the ambiguous point between security and privacy. Digital surveillance requires high-tech digital technology infrastructure, competent, trained human resources, programs and practices. As can be understood from all these data on surveillance and control, the only organized and institutionalized legitimate body is the states; It is seen that they use and trust similar mass surveillance mechanisms regardless of hybrid, authoritarian and democratic country. Therefore, it can be said that mass surveillance is a universal policy whose scope and legal parameters do not depend on the type of regimes.

Artificial intelligence-based digital surveillance systems also provide opportunities for totalitarian and authoritarian mechanisms that want to collect power and information in one hand, rather than democracy that shares information processing and decision-making power among many institutions and individuals. The power of authoritarian regimes in the 20th century, and their desire to collect all information in one place, has become possible thanks

to artificial intelligence today. Artificial intelligence, which makes it possible to process a huge amount of information centrally, the more the amount of information, the higher the efficiency received, and machine learning works better [28]. Therefore, artificial intelligence-based surveillance technologies also serve mechanisms that cause authoritarianism. 49 Surveillance systems are always possible and used by the authorities for good as well as bad purposes. If a state uses surveillance technologies with good intentions, it can turn into a system that is very beneficial to the individual, society and even humanity. The same big data algorithms, in authoritarian, totalitarian governments, malicious uses, such as Orwell's description, can cause the lives of all individuals to be turned into a dungeon. It may even exceed Orwell's, and an absolute surveillance based on not only observing the speech and movements of the individual, but also infecting the individual's body and recording inner experiences, may find a place for itself in the future of humanity. The argument "what's wrong with those who have nothing to hide" to the attitudes developed against surveillance mechanisms is also used to legitimize security policies. With this discourse, while individuals who are against surveillance mechanisms are criminalized, surveillance mechanisms are also legitimized on the basis of the whole society, claiming that security policies are the only solution. It is still a mystery where the digital transformation process the world is going through will evolve. States or large corporations independent of political authority, as in the case of China? or politically organized democratic societies that will dominate the digital world of the future still remains a mystery. The chance of humanity to win this fight is a mystery, so either it will be enslaved under the domination of digital technologies or digital technologies will make humanity more free. Therefore, this will be the biggest handicap that will affect the individual.

2.1.18 Immigrants

Immigrants constitute one of the most fundamental problems of our time, and in this period, which is called the age of migration (Castles and Miller 2003), human movements have become global and have affected almost all states on a global basis. In this human mobility, which is the target of developed countries, it consists of a combination of emigration, immigration and transit countries. Migration is now at the top of the agenda of the international community and many countries and has become globalized. Although migration movements are globalized, they are also tried to be prevented by restrictive

mechanisms. Especially after 9/11, concerns about terrorism strengthened the tendencies stating that immigration should be considered within the scope of security and initiated the process that brought the securitization policies to the fore. The trends in restricting immigration, preventing security and threats have gained importance and brought about the proliferation of restrictions and more surveillance mechanisms for immigrants. As a result of these, preventing migration has become an important goal. Borders between European countries and surrounding countries are structured by tightening surveillance and control channels from sea, land and air through Frontex. 4.1. Although there is no single and comprehensive theory that can explain migration, sociologists have developed various theoretical models based on different concepts and assumptions, and multi-axial, different causality and different forms of inquiry such as individual, household, national and international have been revealed. Migration is the process of moving individuals or communities to different places from the places where they live due to economic, political or social events. Migrants are individuals or communities who leave their place of residence and go to another place for settlement purposes, for the purpose of settling in the country. Migration can be described as a geographical concept and describes the resettlement of individuals to a different city or rural areas from where they live (TDK). Migration is the individual and mass, compulsory or voluntary settlement in the administrative borders of another geography due to natural, political, economic and social reasons. It may be due to compulsory reasons such as natural disasters, exiles, internal conflicts, political pressures or wars, as well as seeking a job, leaving the geography where life is lived with the hope of a better life. Migration is a population movement in which an individual moves, regardless of its cause, structure and duration. Crossing a national or international border, or moving within a country, individually or in groups. This includes individuals and groups moving for different purposes, including family reunification, economic migrants, refugees and displaced individuals [29].

Although there is no universally accepted definition for immigrants at the international level; Migrant is an umbrella term describing individuals who have moved away from their place of residence permanently or temporarily due to various reasons, within the borders of a state or outside an international border. However, legally, the word "immigrant" has different definitions in the international arena. The media and international organizations perceive and

use the word "migrant" to include all immigrants, including refugees. On the other hand, some international institutions and organizations use it to include asylum seekers and refugees. The concepts of immigrant, refugee and asylum seeker are an important distinction. Those who have fled their country for fear of persecution are called refugees, while those who have applied for refugee status and whose request has been processed are called asylum seekers. Immigrants are people who migrate to find a better life, find a job, get a better education or be reunited with their families in other countries. In this study, the word "migrant" is mentioned in the media and international organizations to include refugees, asylum seekers and irregular migrants. Refugees are in a special status and are subject to legal protection by the 1951 Refugee Convention and the 1967 protocol. UNHCR, governments, and humanitarian organizations interact with people who have been granted refugee status because it is dangerous to return to their homes. In Turkey, international protection statuses as refugees, conditional refugees and secondary protection are applied, and residence permits are given in the places determined within this scope. Secondary protection is the status given to foreigners who do not qualify as refugees or conditional refugees, but who are considered to be persecuted in the country of origin or country of residence. Irregular immigrants are also defined as the process of not leaving the country they are in or staying in that country illegally or leaving that country illegally, even though they have entered the borders of a country illegally or entered legally within the specified period. Irregular migrants are positioned as one of the most important problems of today as separate stages as source country, transit country and destination country. Irregular immigrants are the person who crosses the borders of the country without fulfilling the procedures by the source countries, the foreigner who enters the country legally or illegally for the transit country and uses the country as a transit point, the foreigners who enter the country illegally by the target countries, and stay illegally. In accordance with the principle of non-refoulement, the 1951 Geneva Convention and its 1967 Protocol prohibit the return of individuals under conditions where their life and freedom are threatened due to religion, race, social group, nationality, political opinion and political affiliation. Under EU law, the Dublin Regulation, EU asylum legislation and all actions under return must not contradict the principle of non-refoulement and the right to asylum. On the other hand, many individuals who do not fall under the definition of refugee may be in danger if they return to their place of residence. Therefore, protecting immigrants against xenophobia, racism,

violence, exploitation and forced labor, not being detained without a legitimate reason and not returning them by force is an obligation imposed on states by international agreements. While the majority of migrations take place within the countries themselves, international migration continues to increase intensively. The rates of international migration, which constitutes a small portion of the world's population, such as 3.6%, are increasing in some regions and countries. More than 88% of the population in the United Arab Emirates is made up of international immigrants. The Henley Passport Index, which is a country ranking on a world basis according to the number of destinations in the world that its citizens can access freely and without a visa, also shows that a country's citizens can also enter another country's borders, and that that country is a developed and stable country, as well as its place in the international community. While citizens of countries with a high level of development travel visa-free to the vast majority of other countries in the world, almost all of them, the restrictions applied to countries with a low level of economic development are increasing at the same rate. This situation also causes the closure of legal migration routes and the formation of irregular migrants. International migration is constantly increasing, the total number of immigrants, which was 281 million in 2020, is 128 million compared to 1990 and an estimated three times more than in 1970. International immigrants, who make up 3.6% of the world population, are estimated to be around 281 million. Despite this situation, only 1 person out of is an immigrant, and the vast majority continue to live in the place where they were born. Immigrants can change the economic, demographic and social structure, as well as create factors that will question the structure of national identity. In this context, some states that accept immigrants integrate immigrants into the system with their multicultural policy, some countries only accept immigrants for labor force, prevent them from granting citizenship by not allowing family reunification and permanent settlement, and in some 54 countries, citizenship is given to immigrants if assimilation is accepted. On the other hand, in some countries, immigrants are seen as the cause of illness, crime and unemployment, while in some countries there is an anti-immigrant discourse with the discourse that they take away their profession, cause housing prices to rise, and put a burden on social service institutions. Again, in countries that accept immigrants, some groups are growing by making politics on the basis of anti-immigration. Although refugees and displaced persons are relatively few among migrants, it is these people who need help and support the most (IOM,

2020). Factors such as the civil wars and the Arab Spring cause difficulties in distinguishing the factors behind migration, and human rights and economic reasons have made it difficult to separate them in this process. As a result, the distinction between irregular migrants has become difficult. It has displaced thousands of people, especially conflicts and internal turmoil in the world, making them refugees, and started a migration process towards safer areas. In this regard, the European Union has long been a center of attraction for immigrants. Looking at the immigrants living in Europe, it varies as those who migrate for family reunification, educated immigrants with professional occupations, transit immigrants and asylum seekers looking for a safe place [30].

which was created by individuals on the move throughout the history of securitization, has become more complex and more complex in the era of migration. In this age, not every individual can go where they want, some doors are kept open and some doors are kept closed in order to never open. Immigrants, who set out with hope, force closed doors and the settled order to change with their grievances, while on the other hand, authorities bring with them a process in which they invest and support more surveillance and control mechanisms. The classical security understandings of states based on military defense and power against threats started to change after the cold war period. The state-centered system has left its place to an understanding centered on the individual. In this process, which started to occur with the effect of globalization, the scope of threats changed and energy resources, climate, war zones and most importantly, immigrants began to be included in the scope of threat. As a result of this, the authorities have started to deal with immigration within the framework of security in order to maintain their existence, maintain and raise the living standards of their citizens, and protect them. The concept of security has become international rather than national by deepening its content. International immigrants, foreign workers, resident refugees, refugees, which were not seen as a central problem until after the Cold War, are mostly looked at within the knowledge of places such as business offices and foreigners' police. International immigrants, whose signs were seen with the oil crisis, but after the cold war began to draw attention systematically. After the Cold War, the disintegration of some authorities, the change of borders, wars and internal conflicts have occurred, causing mass slaughters and migrations. The unpredictability of the threats and asymmetric warfare, which started after the Cold War and reached its peak especially after September 11, started to come to the fore. Where, when and how a threat may occur is manifested as unpredictability,

and threats to the future are seen as asymmetry, threat, war. Organized crime organizations and terrorist networks are seen as the main security threat of the EU. Such threats, taken within the scope of both internal and external security threats, encourage technological responses by nature. The assertion of unpredictability as asymmetrical characters and unpredictability, asymmetrical, not like us and unpredictable, unknown when it will happen, has made technological surveillance, information gathering and processing systems much more useful. On the other hand, studies are carried out in this context in order to find out how to stop, what is necessary for action or on-site intervention, analysis and picture of threats for research and at the same time to make those who do not know known. Information and surveillance technologies try to know in order to present a picture of threats, internal and external threats to eliminate risks, and to make the unknown less threatening. Anti-immigration started to rise after far-right groups responded to the threat to the European identity that they developed against immigrants in the 90's in the European Union, the subsequent September 11 terrorist attacks and the events that followed were legitimately evaluated within the scope of securitization. paved the way. Although the securitization discourses developed against immigrants came to the fore with the number of immigrants reaching the peak in 2015, it is seen that they have been openly addressed by the European Union since 2003. After the Schengen Agreement was signed in 2013, it is seen that international migration was handled within the scope of securitization, and surveillance and inspection practices began to be structured within this scope. While the European Union was removing its own internal borders and making them free, there was a process in which they started to develop and activate surveillance and follow-up mechanisms for the strengthening of their external borders. The fact that the immigration departments of the interior and police units play various important roles in the regulation of immigration has made immigration problematic. Because producing security information and suggesting security measures is a requirement of the police profession. The fact that such units play an important role in the issues related to immigrants causes asylum to be viewed as a security issue, regardless of immigrants, refugees and asylum seekers, instead of perceiving asylum as a human right. Illegal, illegitimate and negative portrayal of immigrants and their politicization also make them a part of domestic politics as a security-related crime. Today, it is seen that the surveillance and follow-up mechanisms of the borders are very strict and strict, but the

policies that do not fulfill the goals of international rights and law declared for immigrants and are pushed to the second place come to the fore. From the perspective of the declared international human rights and the European fundamental requirement, the surveillance and control mechanisms of the borders pose great difficulties for the immigrants. Migrant tragedies and deaths that have been going on for years at the borders, ill-treatment, exclusion threaten the values on which humanity rises and liberal democracy, and encourage xenophobic formations and tendencies. Immigrants are the most important issue affecting European politics in recent years, and in this context, discussions of refugees, asylum and migration take an important place. Immigrants, especially irregular migrants, is one of the issues that the European Union has been dealing with for many years, both economically and in terms of security. The European Union has long been a center of attraction for immigrants in terms of economic, political and, most importantly, democratic values (Ramli, 2021). The European Union has implemented a series of regulations and practices in terms of tracking and surveillance of immigrants with economic, political, social and cultural effects. In the process leading to the formation of the European Union, firstly, with the participation of Germany, France, Belgium, Luxembourg, Italy and the Netherlands 57, 1951 European Coal and Steel Community established. The Community, which was named the European Economic Community by signing the 1957 Treaty of Rome, which allows the free movement of labor, goods and services, was named the European Union with the Maastricht Treaty in 1993. The Treaty of Rome is also one of the most important turning points in the history of the European Union, with the idea of eliminating borders for the creation of a common market. As a successful result, enlargement policies were implemented. European Union, Germany, Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Cyprus, Croatia, Netherlands, Ireland, Spain, Sweden, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, Poland, Portugal, It consists of member states such as Romania, Slovakia, Slovenia and Greece. The European Union, which has a legal system that binds all member states and their citizens in the same way and extent, was established by the member states with international agreements, has a supranational structure, and the decision-making authority in some areas has been given to the EU by the member states. A common market was established, which ensures the free movement of goods, services, capital and persons. When we look at the policies of the European Union towards immigrants; With the Rome Treaty, free movement of labor was granted in 1957, and

workers and their families were given the opportunity of free movement in 1968, while the TREVI group was formed against criminal elements in 1976, and most importantly, the Schengen Agreement was signed in 1985, which brought the opportunity for short-term free movement. While the possibility of free movement was provided with the Single European Act in 1986, the internal borders of the EU member states were abolished in 1992 with the Maastricht Treaty, and a five-year transition target plan was determined with the Amsterdam Treaty in 1999 to determine policies for immigration and asylum policy. Again in 1999, at the Tampere Summit, the EU was given authority and responsibility on migration, and a decision was made to cooperate with the European Asylum Program and the countries where the immigrants came from. With the EU Charter of Fundamental Rights, it was accepted in 2000 to define the rights of all individuals in the union, including immigrants. The Schengen Agreement, which is an initiative of the European Union to create a safe space, aims to remove the controls at the borders between the member states and to develop a common border management system at the external borders, and is essentially a identification and classification process. In this context, the Schengen Agreement brings with it a spatially and temporally limited free movement of third-country citizens to the European Union border entrances. Within this structure, all states other than the member states of the European Union are defined as third states. Fortified continents such as Europe, which has fortified external borders and needs cheap labor, liberate their internal borders and protect their external borders with very tight mechanisms. On the other hand, they implement practices to maintain global flows without disrupting the current world economic order, to provide cheap labor to residents, and to secure borders more against those who do not want to (Franko, 2005). The challenge here is how to distinguish between 'good' and 'bad' global movements, rapid checks for those who qualify for entry, and the fastest and safest way to detect forged documents or intruders. Within the scope of evaluating the beneficial potential of migration flows, it is also to facilitate the movements of certain groups of people that will benefit the economy with practices such as the qualified immigrant program. Therefore, the aim is not to close the border, but to tame 'mobility' by managing it efficiently, effectively, and to channel them effectively in certain situations [31]. On the other hand, mobility has become more complex and globalized, and possible cross-border and transnational threat networks such as terrorism, secret migration, drugs, human trafficking have brought the fight

against global threats beyond national borders, and cooperation with non-state actors in the task of border control. , 2005). A wide range of technologies are used as part of these measures to prevent security risks and potentially risky persons before they have a chance to enter national territory. Similar logic is used to prevent immigrants from reaching EU borders. Overseas refugee camps established outside EU territory can be considered in this context. Digital technologies also play an important role in regulating mobility within the European Union and preventing unwanted elements, irregular migrants and illegal movements. Monitoring and surveillance systems based on digital technologies, positioned within the scope of the protection of EU borders, establish the distinction between insiders and outsiders, which is a function of traditional state borders, across the EU. This structure is in favor of the citizens of the union and against the foreigners, because the collection of information by technological means actually targets the second group, and it is a structure that is based on digital border tracking and classification. Immigrant flows to the European Union also change according to war, internal conflict and economic conditions in the world, and such situations affect the density of immigrants. As a result of the Arab Spring and the war in Syria, the flow of migrants, which was more than 1.8 million in 2015⁵⁹, decreased by 92% to 142 thousand in 2019. At the same time, the harsh practices of the European Union within the scope of surveillance and monitoring of borders, agreements and aids with third countries and countries of origin cannot be denied. Inbound migration flows are also uneven across EU member states, and some border states are much more affected by migrant flows. Millions of people around the world continue to have to leave their habitats due to conflict, persecution and economic reasons. The inadequacy of legal means in the European Union has pushed the displaced people to different paths. Immigrants reach the borders of the European Union after a dangerous journey, risking the lives of their families for a safer and better life. While thousands of people die on this journey for a safe environment, the survivors experience the pain of witnessing the loss of their loved ones before their eyes. The lack of legal means convicts women, children and families to human smugglers, causing them to embark on this dangerous journey. In this context, the number of refugees who reached the shores of the European Union in 2015-2018 was around 1.8 million and most of them embarked on this dangerous journey due to persecution and conflicts. To reach the European Union, only 5,096 people died in 2015, and 14,281 people drowned in the sea between 2015 and 2018. While the great migrant crisis in 2015 revealed how unprepared the

European Union was, the entry of hundreds of thousands of immigrants into the European Union without proper registration caused political debate, and the public response to the growing anti-immigration response was anger. With Frontex, which has been restructured with securitization policies, borders have started to be protected more strongly. However, with the new migrant crisis in Afghanistan in 2021, it is seen that the main problems continue. More than one million non-EU immigrants entered the EU member states in 2015, especially from the southern and eastern borders. The European Union has been dealing with the migrant crisis ever since. Masses of continent-wide immigrants seeking residence and struggling to gain refugee status have become a politicized issue across Europe. The European Union has affected EU integration operations as well as the collapse of systems governing human movements. While the displacement of immigrants caused great controversy, on the other hand, the Dublin System was clogged and came to the point of collapse. The direct or indirect support of some member states' securitization strategy, including the institutions and organizations of the Union, also complicates the integration process of immigrants into European societies. On the other hand, policies to restrict immigration are increasingly politicizing immigration as a danger. Immigrants have been securitized by presenting them as a threat to the cultural structure, public order and labor market stability, with the emphasis on living conditions on the basis of immigrants, racist, xenophobic, especially anti-immigrant movements and parties in the European Union [32]. On the other hand, while it damages the values of solidarity, social integration and cultural identity discourses on which the European Union is built and promoted, it also affects human courtesy and public order (Huysmans, 2000:771). The securitization of policies regarding immigrants and the policies that exclude individuals by categorizing them and seeing them as a threat to cultural values and social structure also contribute to the continuation of radical discourses and make it difficult for immigrants to integrate into the EU. Immigrants, who are women, men and children from many different places, are not a homogeneous group, and there can be profound differences in their digital literacy, ideological positions, experiences, demographic characteristics as well as cultural, linguistic and social competencies. In addition to all these, in recent years, the politics of blaming immigrants has led to the increase in incidents such as hatred, humiliation and exclusion, causing these behaviors to be taken for granted by the society and, as a result, to cut off solidarity with

immigrants. Attacks, prosecutions, sanctions and politics based on intimidation leave immigrants even more vulnerable. Such problems have become more difficult than problems related to the right to housing, access to legal aid, and language. Various measures have been put forward in order to restrict and prevent the increasing irregular migration movements in the European Union in 2014 and later. While return agreements were made with third countries on the one hand, border surveillance and control works were tightened and the immigration phenomenon was securitized, thus reducing irregular migration to a large extent. The European Union has started to develop various measures in line with the general aim of limiting irregular migration, especially in response to the migration flow that reached its peak in 2015, all means were used, including militaristic methods, securitization and externalization of migration. On the basis of the European Union, the presentation of migration as a risk and then a threat has justified its increasingly security-oriented policy against immigrants. With the legitimization of security policies, it has begun to be used, including maritime operations, army deployment, unmanned aerial vehicles, satellites, biometric devices and equipment, under the leadership of Frontex, to secure its borders and repel immigrants. Migration to the European Union from different parts of the world, which poses a security risk and causes human tragedies, is one of the most controversial issues in recent years. The European Union has accelerated its efforts to secure and militarize the borders within the scope of the fight against immigrants. Migration routes at borders, especially sea and land routes, have brought along the equipping and deployment of airways with paramilitary and military forces, vehicles and equipment to prevent migration, and the militarization of migration control. Frontex, which was created to manage this process, also ensures the intensification of cooperation between the law enforcement agencies of southern and northern European countries, and is supported both in terms of budget and personnel. In addition to strict border policies and militaristic practices, as a result of agreements and studies with third countries, oak countries and transit countries such as Turkey and Libya, the flow of immigrants, whose number exceeded 1.7 million in 2015, decreased to 123 thousand in 2019. The procedures for returning immigrants cause arbitrary treatment of certain persons, and efforts to solve the problem are insufficient. The arrest and deportation of immigrants is not an effective solution. It raises the issues of constitutionalism and fundamental rights. Although militaristic and police measures have reduced migrant flows, they are doomed to failure. Prohibition policies do not prevent immigrants, but also bring

about human smuggling and the use of alternative ways and channels, making the solution more difficult. Even if migration is reduced using militaristic methods, it cannot be stopped because migrants always find a way. It is not because Germany is closer or richer than other countries that immigrants choose to immigrate to Germany first over Iran, Arabia, Japan, or Russia, but rather a better track record of human rights and welcoming, accepting, and hosting immigrants. should be seen as a reason [34].



3. MATERIAL AND METHODS

3.1 APPLICATIONS OF BIOMETRIC SYSTEMS

3.1.1 Border Tracking and Surveillance

Mechanisms Especially since the middle of the 20th century, the places where border controls were made and the physical borders did not coincide, and the position of the borders began to transform as a result of the emergence of new mobility opportunities. Cross-border movements and crossings have started to be made over new transition routes such as airports, rather than the end points of physical border lines of states, and the structure of physical borders has also changed, and physical walls have been replaced by technological structures equipped with technological barriers, databases, and digital-based devices that track and monitor on land and sea. left [35]. Surveillance and monitoring of the borders of the European Union is one of the most important issues in the eyes of the EU. Budgets are allocated for effective and desired organization of migrant movements, prevention, back agenda, integration of accepted ones, prevention of immigrants to countries of origin and third countries. The environment created and created especially after September 11 has caused immigrants to be seen as a security problem by authorities and societies, and policies have been developed accordingly. The European Union has also developed and implemented security-oriented policies for immigrants. Among the member states of the European Union, it is seen that the security-oriented practice towards immigrants, especially after 2014, has come to the fore. While the institutions created within the scope of these practices act as a shield against immigrants, it is aimed to increase cooperation between the member states of the European Union and to act as a bridge. Security-oriented institutions and applications created for border security Frontex, Eurodac, Eurosur, SIS II and AFIS are at the same time tracking and interim surveillance tools and consist of a structure where information collected about immigrants, including biometric data, is archived and these archives are used within the framework of banoptic surveillance applications. Therefore, immigration policies consist of not only laws and policy measures, but increasingly technologies [36].

3.1.2 Information System

The basic mission of Eu-LISA, which develops solutions and operational management of surveillance technologies used in the implementation of border management, migration and migration policies, is to support EU policies and practices through secure technology. Eu-LISA (The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice) It provides the management and organization of technologies related to the control of In this context, it manages Visa Information System (VIS), Schengen Information System (SIS II), Eurodac systems 64 dealing with visas, asylum claims and information sharing. On the other hand, EU information systems such as eu-LISA Entry-Exit System (EES), European Travel Information Authorization System (ETIAS), European Judicial Registry Information System, Third Country Nationals (ECRIS-TCN) provide technological support, better access to data and EU level carries out projects aimed at providing identity management. Eu-LISA Agency works in close cooperation with EU institutions, agencies and EU member states, especially in the fields of justice and home affairs. In this context, it cooperates with institutions such as Frontex, Europol, EASO, European Union Law Enforcement Training Agency (CEPOL), European Union Network Information Security Agency (ENISA), European Union Judicial Cooperation Unit (Eurojust), European Data Protection Supervisor, Fundamental Rights Agency (FRA). works in close cooperation. Eu-LISA Agency is responsible for the operational management of Eurodac, Visa Information System (VIS) and Schengen Information System (SIS II), which has an important place in the surveillance and follow-up of immigrants, and also works on their development and operation [37].

3.1.3 European Dactyloscopy Database (Eurodac)

The EURODAC (European Asylum Dactyloscopy Database) European Asylum Dactyloscopy Database, managed by EU-LISA, is an information technology system established for archiving and processing digitized data, genetic fingerprints of immigrants. Eurodac's digital archive data is used in the evaluation of new asylum applications to the European Union. Eurodac, which became operational in 2013 as a result of the work carried out within the Schengen Information System to establish a data bank for immigrants, is a central database system that processes digitized fingerprint data of immigrants, with the main

starting point of the Dublin contract being the activation. Member states use the Eurodac system to compare existing immigration data, which has been archived, while entering new fingerprints. Law enforcement, Europol, also has access to the system, which helps identify multiple asylum applications. Within Eurodac, the Automatic Fingerprint Identification System (AFIS) system is used for obtaining, archiving and analyzing the fingerprint data of immigrants. The digital imaging system AFIS provides automatic recognition and control of the fingerprints of immigrants, thanks to its biometric identification methodology. Eurodac is a database of fingerprints of foreign nationals, especially asylum seekers, established by the Dublin Convention. The main purpose of Eurodac is to prevent people from seeking asylum in 65 various European countries [38,39]. Eurodac, which has an important function for the common asylum policies of the European Union, is also seen as one of the most successful systems of the union. The main purpose of Eurodac is to apply to or prevent immigrants coming from countries such as Greece, Spain, Italy, Poland, which are the EU border countries and also receive the most immigration, to apply to the countries they want or to prevent them from leaving, even if they have come to the countries they want, by detecting them from their fingerprints and making their first entry. their repatriation to countries. In this context, fingerprints are taken from incoming immigrants and entered into Eurodac as data. When immigrants apply to a second country, a comparison is made on the system side, and if there is a fingerprint, it is ensured that the fingerprints are sent back to the country where they were originally taken, within the scope of the Dublin Regulation. Member states can also implement various applications. Germany has allowed immigrants' identity information, including fingerprints and country of origin, to be archived in a centralized structure and accessed by all government agencies. Within the scope of increasing and diversifying the data received from immigrants, it was decided to upload facial images, passport and identity card details, as well as fingerprints to the Eurodac database, and to carry out studies to include immigrant children under the current minimum age of six. Amnesty International and human rights organizations have submitted their demands to the European Parliament, containing their concerns that Eurodac will turn into a mass surveillance tool within the scope of immigrants [40]. The system, which fulfills an important function for the member states of the Union, causes immigrants to resort to alternative and dangerous routes, especially in order not to be registered in border countries. Immigrants who want to give fingerprints to the authorities of the countries they want to stay

in in order not to come back to the border countries are condemned to alternative routes and human smugglers, taking the risk of life. The Schengen Agreement, which is an attempt to create a safe space, is essentially a identification and classification process aimed at removing controls on the borders between member states and developing a common border management system at the external borders by creating an area of freedom, security and justice [41]. European border security depends on various transnational information flows and technological zones, in particular the Schengen Agreement and the Dublin Convention, which deal with asylum issues. Schengen Information System (SIS), which is the most widely used data and information sharing system for border surveillance in the European Union, was established in 1995, updated in 2013 and 2018, and named SIS II. The Schengen Information System (SIS) derives from the Schengen Agreement and its purpose is to essentially eliminate the internal borders of the EU while coordinating and strengthening the external borders of the EU, especially through better cooperation and information exchange within the scope of police measures. Within this structure, all the states other than the member states of the European Union are defined as the third state, the persons other than the citizens of the member states are defined as foreigners, and various regulations have been made regarding free movement and short-term mobility in the union geography. In this context, the Schengen Agreement brings with it a spatially and temporally limited free movement of third-country citizens to the European Union border entrances. The Schengen Information System (SIS), which has an important place in the management and security of borders, provides data exchange between visa centers, customs and border security. It helps the members of the European Union to provide internal security without the control of internal borders by providing cooperation in three areas: cooperation in border control, cooperation in law enforcement, cooperation in vehicle registration. Within the framework of follow-up, surveillance, return decisions, entry bans of immigrants are processed into the system, biometric data such as palm prints, fingerprints, facial images and DNA (Deoxyribo nucleic acid) will begin to be taken. By providing system integration of European Union institutions and authorities, more data is shared with the member states in a complete and secure manner via SIS, while operational institutions such as Europol and the European Border and Coast Guard Agency use the SIS system within the scope of combating migration. All member states are able to search, use AFIS, search on the basis of fingerprint

in SIS. SIS II, which is the main element of the control and surveillance mechanism of the European Union immigrants, functions as a news network, and all kinds of illegal processes, especially the missing, wanted persons, foreigners whose border entry is prohibited, are transferred to the data system using biometric digital technologies and monitored [42]. It can be said that the database created in this context has a great function in the surveillance and follow-up of international crimes and immigrants, especially irregular immigrants. According to the data of SIS, the system, which contains approximately 91 million records at the beginning of 2020, was accessed 6.7 billion times and around 284 thousand hits were achieved. A warning system is created by recording the data of individuals who are deemed to be risky or prohibited from entering the union borders with the initiative of the member states, by recording them in the SIS database. SIRENE offices of member countries carry out transactions related to the data transferred to the system. In this context, the Schengen Information System, especially the collection and storage of data for third-country citizens, where the presumption of innocence is violated, and discrimination in some EU countries cause legal and humanitarian debates. As of December 2021, the infrastructure has been prepared for more functional use of biometric data such as facial images and DNA profiles of missing persons, palm prints. The vast majority of personal data kept in the Schengen Information System since its inception consists of data belonging to third country citizens. SIS and its continuation SIS II, in this context, have the right to privacy, data protection, freedom of movement and discrimination.

3.1.4 Ground Observation

instruments have been designated as the sole contact point of Frontex, Copernicus border surveillance services for the European Ground Observation Program (Copernicus) since 2015 [43]. In this context, Copernicus data; It reaches and uses within the scope of surveillance of borders, tracking, mapping, risk analysis and management of operations for the surveillance and follow-up of immigrants. Copernicus data, which Frontex states, used for better monitoring of immigrants, search and rescue and the fight against cross-border crimes, has an important place in the surveillance and tracking process of immigrants. Within the scope of security practices, Copernicus provides services in three main areas: support for EU External Action, maritime surveillance and border surveillance, in order to support the policies of the European Union, to improve preparedness, crisis prevention and response.

While Copernicus provides services to EMSA within the scope of maritime surveillance activities, Copernicus provides services to the European Satellite Center (EU SatCen) of the Security Service's Support for External Action (SEA), providing geographical information about EU institutions and International helps stakeholders [44]. With the aim of border surveillance, Copernicus aims to increase the internal security of the European Union, fight cross-border crimes, and prevent immigrant deaths at sea. Within the scope of the monitoring and surveillance of immigrants, all kinds of transactions regarding the state of the borders of the European Union are transferred to Frontex via EUROSUR in real time (Copernicus, 2021). The Copernicus Border Surveillance Component uses satellite data for georeference and environmental measurements in addition to air, sea, and ground-based surveillance systems. It serves based on the processing of environmental data collected from Copernicus observation satellites and on-site sensors. Within the scope of Copernicus Border Surveillance; It includes services such as front border surveillance, mapping maritime interest surveillance (AoI), ship detection and reporting service, ship anomaly environmental information service, wide area front border monitoring, ground surveillance (EO) reconnaissance, cross-border crime surveillance. Within the scope of land borders, settlements surveillance; Official and informal places such as administrative borders, border crossing points, cities, suburbs, rural areas, official reference buildings, refugee camps, temporary housing are monitored. Within the scope of transportation infrastructure surveillance; Infrastructures related to transportation networks such as roads, rails, paths, railways, bridges, crossings, train stations, ports, airports, helipads, checkpoints, road blocks, border crossing points are monitored. Industry and public services; Industrial facilities such as power plants, power lines, quarries, landfills, mines, storage areas are supervised [45]. Height; Monitoring of places such as land surface, numerical elevation for ocean surface is carried out. Points of interest; Surveillance is carried out at a specific location that may be useful in the context of crises or otherwise important for security reasons, such as schools, hospitals, places of worship, institutional and administrative buildings, diplomatic buildings. Hydrography; Monitoring of natural and artificial water features, such as streams, rivers, canals, lakes, reservoirs, water bodies such as coastlines, drainage network and suitability for embarkation is carried out. Within the scope of maritime border surveillance; Geographical surveillance system, Ground and Satellite Automatic

Identification System (AIS) serve in the surveillance and tracking of marine vessels. AIS consists of a maritime broadcast system that includes reports containing the identity, location and route of the ships and cargo information. Ship traffic service (VTS); Marine traffic is monitored based on ship traffic monitoring by coastal radar networks. Ship Monitoring system (VMS); It consists of a satellite-based ship tracking system that provides information about the ship name, location and activity. Long Range Identification and Tracking (LRIT); It consists of a global ship identification and tracking system based on communication satellites. In maritime border surveillance, data such as patrol boats, airborne MPA, RPA and various radar, electro-optical sensors mounted on land surveillance stations, wind, waves, atmospheric parameters are used [46].

3.1.5 Travel Information and Authorization System

The European Travel Information and Authorization System has been established for the purpose of pre-registration and digital monitoring for the purpose of assessing the security or irregular migration risks posed by visa-exempt visitors traveling to the Schengen area before arriving at the border. ETIAS also establishes a watch list for suspected persons or persons for whom there are factual indications or reasonable grounds based on an overall assessment of the person. The European Travel Information and Authorization System, which is part of Frontex, was established in 2018 and will be operational in 2022 [47]. There are approximately 1,885 official external border crossing points in the European Union and it is estimated that while approximately 565 million crossings were made in 2014, it will increase to 887 million by 2025. It is estimated that one third of these transits will come from visa-exempt countries (Frontex, 2021) [48]. Within this scope of, visa-exempt third-country nationals will be evaluated against irregular migration, public health and security risks. Applications will be subjected to automatic artificial intelligence processes with Frontex, Europol, EU information systems and all other relevant institutions and Interpol databases. Applicants' personal data will also be automatically checked against the new watchlist and certain risk indicators, and will be subject to special rules on an algorithm that will make it possible to identify travelers who fit predefined risk profiles [49]. Personal data such as age, gender, nationality, residence will also be used in risk analysis. Again in this process, digital automation applications based on artificial intelligence and machine learning will come into play under the leadership of eu-LISA [50]. Strengthening the internal security of the

Schengen Area, knowing much more about travelers, tourists who are exempt from visa requirements entering the EU, will support security screening and risk assessment, and will also be an important step in the digitalization of European border management. The European Travel Information and Authorization System entered into force in 2018 and will be operational by the end of 2022 [51]. Eurosur, which started its activities in 2014 with the aim of combating cross-border crime, combating irregular migrants and preventing the loss of migrants at sea, is a data and information exchange system. The backbone of the European Border Surveillance system (Eurosur), which is the responsibility of Frontex, consists of units responsible for border control established by each member state. The main responsibility of these units is to serve as a center for border surveillance, coordinating surveillance activities and information exchange at the national level. These units collect local and national information about immigrants, illegal crossings, and criminal activities and provide a national picture, on the other hand, this information is shared with Frontex. By synthesizing data and information from these units and other EU institutions and organizations, Frontex provides analyzes and intelligence information about borders for the European Union and member states, while providing information in preparation for the operations to be carried out [52]. In addition, Frontex provides information gathered from satellites and other surveillance tools at the European level. Fusion Services uses optical and radar satellite technology to locate vessels with immigrants. The service includes up-to-date technologies, algorithms, software, precise weather and oceanographic forecasts, and is used automatically for vessel tracking, location detection and anomaly detection. Within the framework of Eurosur Fusion Services (EFS), Multi-Purpose Aerial Surveillance (MAS) offers real-time surveillance to EU institutions and member states. Collaboration with the European Maritime Safety Agency (EMSA) and the EU Satellite Center (SatCen) is also being carried out to obtain such data [53]. In order to carry out the necessary procedures in different border regions, the maritime and land borders of the member states of the external borders are divided into various sections. A low, medium or high impact level risk factors for illegal situations, border crossings have been assigned to each of these border sections. Reducing risks is the responsibility of the member state, but Frontex can step in only in high-risk situations. All kinds of technological tools, equipment and vehicles are used to monitor the sea and land borders, and extensive surveillance and control work is carried out

especially at the southern borders of the EU. Every year, thousands of migrants try to reach the EU by sea, often traveling by boats that are dangerously crowded and inconvenient. Frontex is obliged to provide technical and operational assistance to Member States and non-EU countries to support such operations that may arise during border surveillance operations at sea. Within the framework of agreements and plans made with Egypt, Libya, Tunisia and Algeria, it provides a communication network for migrant movements and the establishment of technical infrastructure and technologies that will enable simultaneous movement. In this context, pre-monitoring is carried out for the purpose of obtaining advance notice, data collection and action and planning for groups that are seen as suspicious or potentially at risk [54]. It was assumed that Eurosur's delivery of aid and rescue to small migrant vehicles in distress would improve the image of border agencies accused of human rights violations. While large budgets are allocated to Eurosur, which is structured with advanced surveillance technologies, the reason for these large budget allocations is claimed by the EU authorities to save the lives of immigrants and safety of life. However, Amnesty International also has concerns and objections regarding the stopping of immigrants before they enter the borders and their return. Frontex takes an active role in anti-migrant operations across the EU and its borders, including across borders, with ships, aircraft, drones, patrol cars and radars. Migration routes at borders, especially sea and land routes, have brought along the equipping and deployment of airways with paramilitary and military forces, vehicles and equipment to prevent migration, and the militarization of migration control [55]. The securitization, militarization and externalization efforts of the European Union had an effect on the decrease in the number of immigrants to a certain extent, but they could not solve the problem. Migration routes to the EU and points of illegal crossings vary widely. The Eastern Mediterranean route is used for sea and land crossings from Turkey. The western Mediterranean route is used for crossings from Morocco and Algeria to Spain or the Spanish enclaves of Ceuta and Melilla. The Western Balkan route is used for land crossings from Greece to Central and Western Europe 82. The central Mediterranean route is used for sea crossings from Algeria, Tunisia, Libya, Turkey and Italy to Malta, while the eastern borders route is used for land crossings from Russia, Belarus, Ukraine and Moldova (Frontex, 2020). Migration pressure on these routes fluctuates due to various reasons such as geopolitical developments, emerging or developing conflicts and increased border controls. It provides huge profits for smugglers from the dangerous journeys of immigrants to the EU union. At

the height of the migration crisis, criminal networks involved in migrant smuggling had an estimated turnover of between 3 and 6 billion Euros in 2015, with an estimated revenue of 190 million Euros in 2019 on Mediterranean routes alone [56]. Migrant smuggling, which facilitates irregular migration towards the European Union, is a multinational business and smugglers from 122 different countries are involved in this organization, both EU citizens and non-EU citizens [57]. Most irregular migrants reach the EU by sea, via Mediterranean routes, under the guidance of smugglers. Very basic life-saving equipment, boats, toy boats or small fishing boats can be used as vehicles for sea crossings. Smugglers with connections in the countries of origin, transit and destination usually stay in the country of final departure. At land crossings through the Western Balkans, migrants cross borders on foot in rough terrain. On the other hand, all kinds of vehicles can be used on this route. Irregular migrants traveling by road travel in dark, airtight vehicles in crowded, inhuman and even life-threatening conditions [58]. For immigrants who want to reach European Union countries, digital technology-based systems are as important as infrastructures such as sea crossings, highways, railways and physical border gates. Applications such as mobile applications, websites, messaging and phone calling platforms, social media, translation services contain many technology resources. Digital-based devices such as mobile phones are vital as they provide access to the news and information source of immigrants, and play an important role both in the planning and orientation of the dangerous journey and in the progress of the next process after entering the borders. On the other hand, digital devices such as mobile phones also pose a threat, and the digital traces they leave make immigrants vulnerable to tracking and surveillance mechanisms [59]. Most of the migrant smuggling cases detected in 2019 were detected in the western Balkan region. Greece continued to be a hotspot for facilitating secondary movements to other EU countries, with large numbers of human traffickers continuing to be detected inland. While 4426 migrant smuggling cases were detected in 83 in 2019, 14218 suspected migrant smugglers were identified [60]. Secondary movements by sea also increased in 2019, mostly in the North Sea, Baltic and Mediterranean (EMSC,2020). On the other hand, with the increasing arrivals to the Canary Islands, the use of small boats to cross the English Channel from air to land and sea routes and via the Central Mediterranean has increased, and new smuggling methods and routes such as hiding irregular migrants in freight vehicles and freight trains have been identified. While larger

groups of irregular migrants have been observed along the Western Balkan route, new less-explored and more risky potential new routes have emerged, such as the sea corridor from Albania to Italy [61]. The vast majority of irregular migrants pass through third countries such as Tunisia, Morocco, Libya, Turkey, Russia, Ukraine, Belarus, Serbia, Albania, Bosnia and Herzegovina before being detected at the EU border. Countries such as Algeria, Moldova, North Macedonia, Montenegro and Senegal are also major countries on the main migration routes used by migrants and smugglers to enter the EU [62]. Coordinating maritime operations in Greece, Italy and Spain, Frontex also coordinates at the outer land borders of Bulgaria, Romania, Poland and Slovakia. Ships and planes are also used in the operation areas, and at the same time, studies on illegal crossings are carried out at many international airports in Europe. Frontex, on the one hand, fights against immigrants, goods smuggling and cross-border crimes, on the other hand, assists the relevant member states in search and rescue coast guard services and readmission operations. Every year, thousands of migrants try to reach the EU by sea, and often travel by boats that are dangerously crowded and inconvenient. Under the maritime search and rescue, assistance obligation, the 1974 SOLAS Convention for the Safety of Life at Sea and the 1979 Search and Rescue SAR Convention, Frontex provides technical and operational support to Member States and non-EU countries to support such operations that may arise during border surveillance operations at sea. responsible for providing assistance [63]. As a result of Frontex's operations with member states, complaints about humanitarian tragedies and the use of disproportionate force and inhumane practices in Ceuta, Lampedusa, and Melilla [64]. With the sinking of the boat carrying immigrants in Lampedusa, Italy in 2013, many immigrants lost their lives, humanitarian tragedies before and after them came to the fore again, and Frontex duties and practices began to be questioned. Especially in 2015, Aylan Kurdi's dead body, which washed up on the shores of Bodrum, made the strict border policies of the European Union come to the fore and questioned all over the world. As a result of this, although a certain softening was observed in the European Union against immigrants, the disproportionate use of force that occurred on the Greek borders in 2020 showed that strict policies continued. Discussions regarding the practices of Frontex in terms of basic human rights and law still continue, and accusations are made that the human rights and values that form the foundations of the European Union and on which they are built are put into the background. On the other hand, in order to shift the flow of immigrants to non-EU regions, the EU has

also signed return agreements with a number of third world countries, using financial incentives, to take back illegal immigrants who came from or lived in these countries. These regions mostly consist of countries with much weaker resources and human rights records than the EU itself [65]. Narrowing of external borders leads to increasing deaths among irregular migrants. Blocking safe routes does not mean that migrants have given up on their plans to enter Europe. On the contrary, immigrants are exposed to even greater risks in taking alternative, more dangerous routes [66]. Operation Poseidon covers Greece's maritime borders with Turkey and the Greek islands. With the Poseidon Operation, the Greek State authorities are supported in order to prevent border surveillance, fight against cross-border crimes, detection of immigrants, interrogation, registration, identification, screening and loss of life. With the Poseidon Sea Operation, on the one hand, the fight against illegal human and property smuggling and cross-border crimes, on the other hand, the Greek authorities are assisted in the coast guard services and readmission operations for the search and rescue of immigrants. Within the scope of Operation Poseidon combating cross-border crimes, Frontex collects intelligence about migrant smugglers, migrant population and countries of origin of migrants in Turkey and is shared with Greek authorities and Europol [67]. With Turkey's opening of its borders in February 2020, thousands of immigrants took action to cross the Greek border to Europe. In this process, Greece's border with Turkey witnessed many human rights violations, including gross violations of fundamental human rights and the right to life for immigrants. Violence at the land and sea borders reached its peak. 85 Greece has made every effort to prevent the passage of asylum-seeking migrants. The European Union also activated the Frontex agency and sent it to help. Greece's refusal of asylum requests, the support of Frontex in pushback and other operations led to discussions that the Geneva Convention's principle of non-refoulement was violated. Frontex's capacity to intervene, monitor the effective functioning of member states' external borders, assess vulnerability, verify whether the member State can effectively enforce EU laws, and identify deficiencies in the management of its borders [68]. The procedures for returning immigrants cause arbitrary treatment of certain persons, and efforts to solve the problem are insufficient. The arrest and deportation of immigrants is not an effective solution. It raises the issues of constitutionalism and fundamental rights. Although militaristic and police measures have reduced migrant flows, they are doomed to failure [69].

3.2 CONVOLUTIONAL NEURAL NETWORKS

Convolutional neural networks are neural networks that contain at least one convolutional processing layer. Convolutional neural networks are optimized for multidimensional data processing. For example, color images composed of two-dimensional matrices, language processing data stored in two-dimensional data, and three-dimensional movies include volumetric images. Local connections, shared weights, coupling and the use of several layers are the four critical elements of convolutional neural networks that use the attributes of real signals [70,71]. In general, convolutional neural networks consist of five different structures: an input layer, a convolution layer, a common layer, a fully connected layer, and an output layer. , Figure 3.1. shows a convolutional neural network architecture.

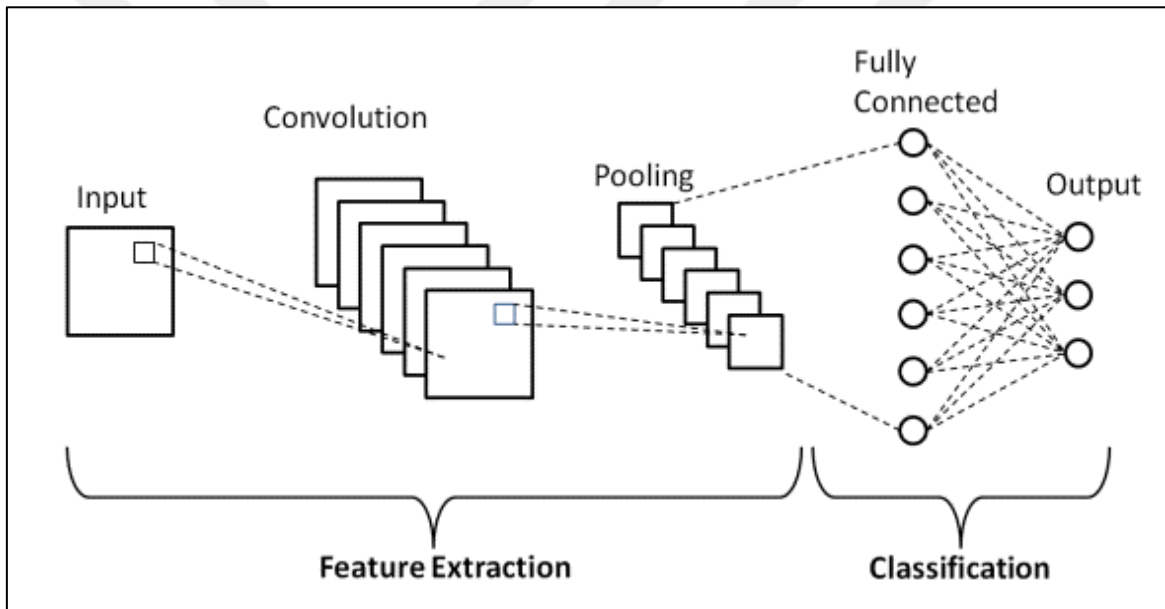


Figure 3.1: Convolutional Neural Network [70].

The convolution layer used in the model shown in Figure 3.1 consists of three components. First, the convolution process is performed on the data received as input. In the second step, a non-linear activation function is performed on the data coming to the layer. In the last step, the jointing process is carried out. Then the incoming data is sent to the output layer. The convolution layer is the first layer that handles the incoming data. A filter smaller than the original image size hovers over the image in the convolution layer, trying to collect certain attributes from these images. Figure 3.1 illustrates the convolution operation applied to a two-dimensional input image. The feature map S is created by applying the w filter to the input matrix x . When w filtering is performed on input x , which has a matrix size of 3×4 ,

a result s of size 2×3 is produced. A feature map is obtained by summing all the cells, after the s results obtained are written to each cell. According to the type of work performed, the activation function, which is one of the process parameters, should be determined correctly [72]. The most commonly used activation functions in the literature are Sigmoid and ReLU. The jointing process applied as the last step, a certain size matrix is hovered over the input image and it performs the operation by taking a sample from the image segment at each position it passes. If we consider the input matrix as $M \times N$ and our wandering matrix is $K \times L$, the output size is reduced to $(M-K) \times (N-L)$. By performing a reduction operation in this way, it reduces the computational cost of the prepared network model. Therefore, it is of great importance for convolutional neural networks [73].

3.2.1 Fundamental Components of Convolutional Neural Networks

Convolutional neural networks convolution layer, jointing layer, activation functions, fully connected layer, loss layer, heap normalization layer and coupling layer It consists of 7 basic structures. These structures are described in detail below. The primary function of the convolution layer is to convolutionally apply the selected filter to the input matrix to extract the required features. The critical parameters for the convolution layer are filter width, number of filters, step and pad size. The filter width value specifies the size and width of the filter element moving across the input matrix. When the number of filters is changed, the number of features in the feature map also changes. The step interval specifies the intervals at which the filter element crosses the input matrix. The fill size is the parameter used to classicize the output size and feed back in various ways [74].

The pooling layer (POOL) is a sampling procedure often used in conjunction with a convolution layer with some spatial variability. For example, maximum and average coupling are unique types of coupling from which the maximum and average values are obtained. The partnership layer is generally used to reduce the transaction cost. There are two most commonly used jointing methods. They will be mentioned in the following section [75].

Max Pooling: In the matrix taken as input, the largest element in the dimensions of our floating matrix, which performs the jointing operation, is output. The realization of 2×2 maximum jointing operation on a 4×4 matrix taken as input is given in Figure 3.2.

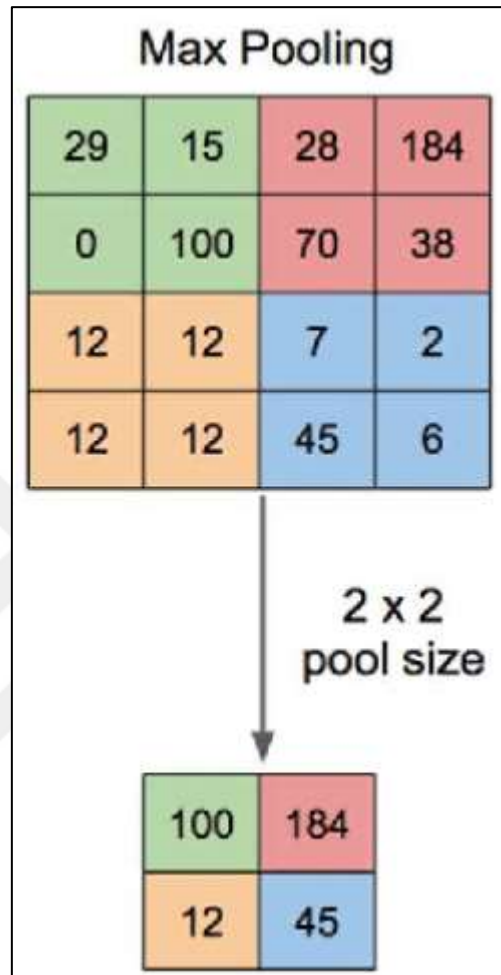


Figure 3.2: Max Pooling [74].

Pooling to Average Value: It outputs the average value of the elements within the dimensions of our floating matrix, which performs the jointing operation in the matrix taken as input. The realization of the 2×2 average value jointing operation to a 4×4 matrix taken as input is given in Figure 3.3.

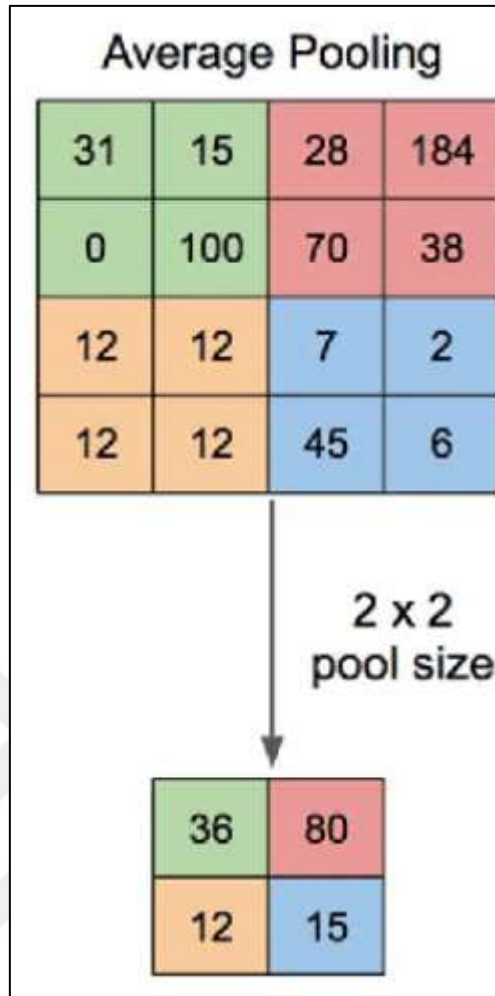


Figure 3.3: Average Pooling [75].

Activation functions are expressed as an operation that gives the result after processing the data received as input in each layer, as an input to the other layer to be processed. It is important for the network used to determine the appropriate activation function according to the characteristics of the processed data. There are two commonly used activation functions called ReLU and Sigmoid.

Sigmoid Activation Function: The sigmoid function is a continuous and differentiable mathematical function that translates numbers between 0 and 1. It has a distinctive "S" shaped curve. The sigmoid function is often called the logistic function or the sigmoidal curve. It is a very common and nonlinear bit activation function.

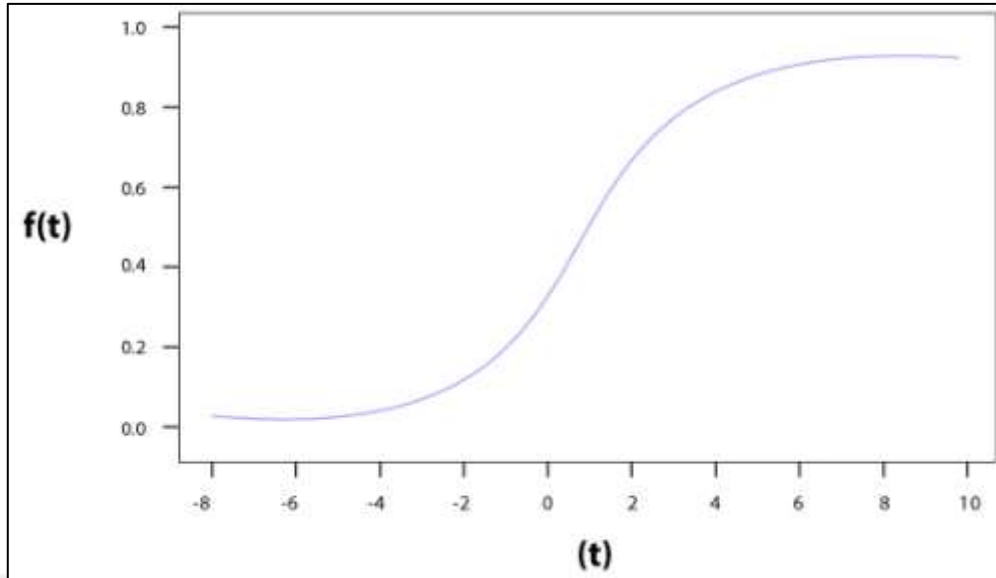


Figure 3.4: Sigmoid Activation Function [72].

Generally, in a neural network, fully connected layer processing is performed after the convolution and coupling layer. The fully connected layer is interconnected with the layers before it. The values from the fully connected layer, convolution and communing layer are multiplied within the values within itself, and the obtained values are biased. In convolutional neural network, the data processed after convolution, jointing, full link layer finally comes to the lost layer. The loss layer calculates the relationship between our dataset and the predicted result of the network we trained on the test data and the targeted result via an error function. It extracts the input data with a probability value for each of the targets it should have, and it is associated with the one with the highest value among these values. The heap normalization layer is the layer where the convolutional neural network is optimized without performing any optimization algorithms. Since the optimization process is performed within the layer, the training phase of the data is accelerated. At the same time, it increases the test performance by stabilizing the used model. The consolidation layer is the layer that properly combines data from different sources. In other words, merging of feature maps obtained from different data is performed.

3.3 PROPOSED BIOMETRIC SYSTEM USING CNN

In this study, new structure of CNN applied to recognize humans using IRIS images. The proposed CNN structure consist from 9 layers which mean it's not contain large number of

layers and processing functions. These layers produce high effective features with low dimension data according to the output of the 9 layers of the CNN.

Then, the output of the CNN layers wired to the several classifiers such as DT, ANN, MLP, RF which are classification techniques applied to classify the labelled data. The flowchart of the model presented in the figure 3.5.

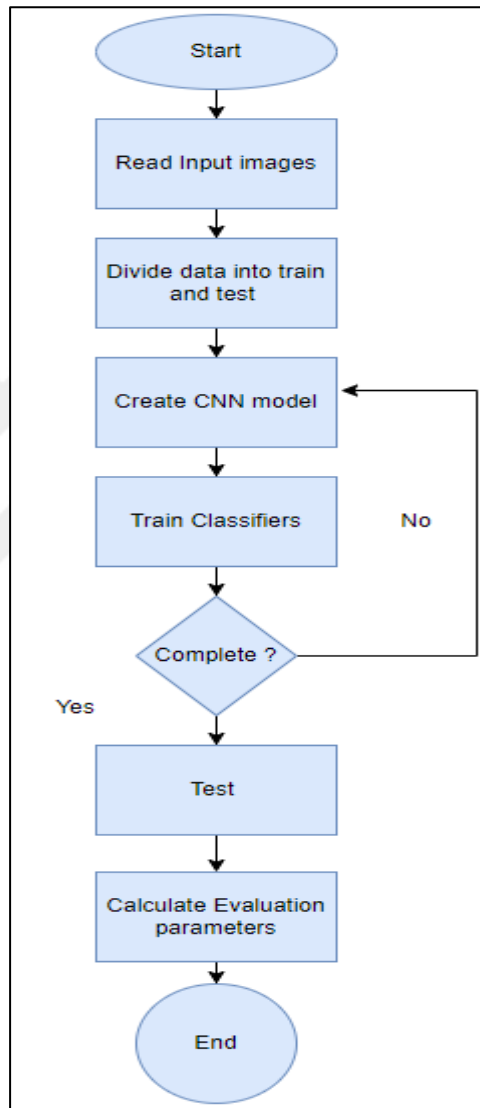


Figure 3.5: Proposed Method [70].

4. RESULTS

4.1 MMU IRIS DATASET

4.1.1 CNN Based Decision Tree Results With MMU IRIS Dataset

The results of this method presented in the figure 4.1.

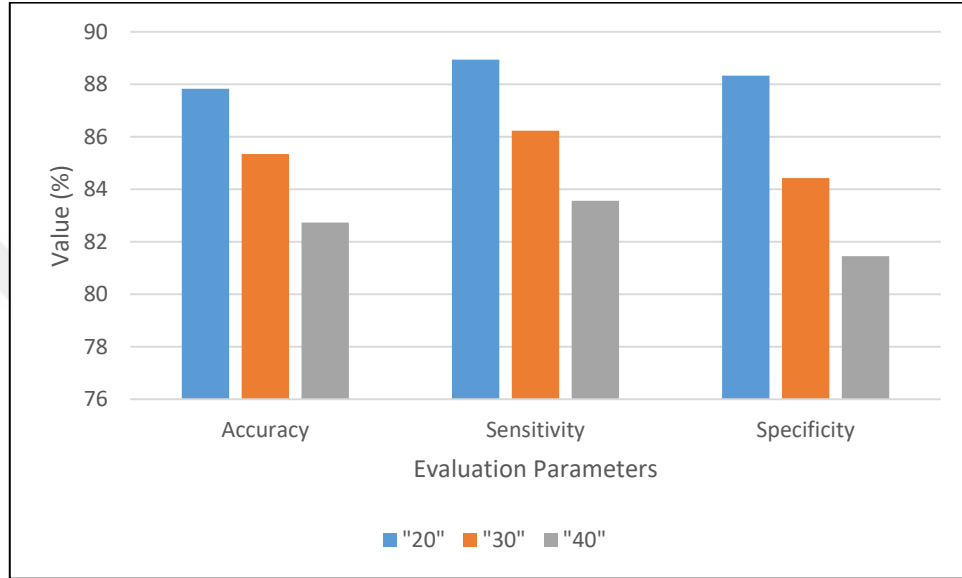


Figure 4.1: CNN Based DT Results with MMU IRIS Dataset.

The figure shows the results of a CNN-based decision tree method for iris recognition on the MMU IRIS dataset. The dataset consists of 20,000 iris images of 500 subjects, and the method was evaluated by testing 20% from the data, 30% and 40%. The results show that the method achieved an average accuracy of 85.33%. This is a good result, and it is comparable to the accuracy of other methods that have been used on the MMU IRIS dataset. The method works by first extracting features from the iris images using a CNN. These features are then used to train a decision tree classifier. The decision tree classifier is then used to classify new iris images.

4.1.2 CNN Based Random Forest Results With MMU IRIS Dataset

The presented in figure 4.2.

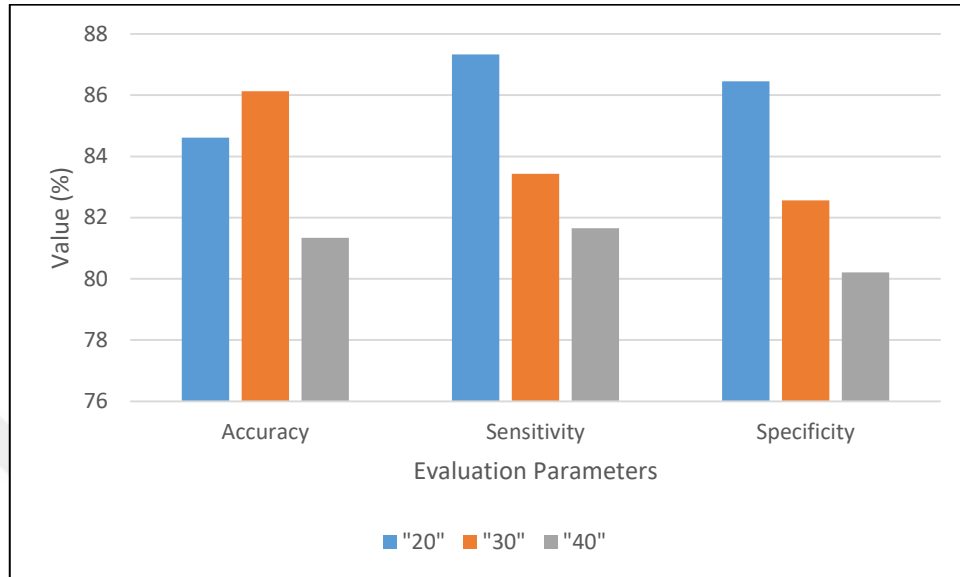


Figure 4.2: CNN Based RF Results with MMU IRIS Dataset.

The figure shows the results of a CNN-based random forest method for iris recognition on the MMU IRIS dataset. The dataset consists of 20,000 iris images of 500 subjects, and the method was evaluated using a leave-one-out cross-validation procedure.

The study evaluated the performance of the CNN-based RF model on the MMU IRIS dataset. The results showed that the CNN-based RF model achieved an accuracy of 93.33% on the training set and 92.67% on the testing set. These results are comparable to the results of other studies that have used CNNs or RFs to classify iris images.

The reason why the random forest method works better is because it is able to learn more complex relationships between the features and the labels. The decision tree method is only able to learn simple relationships, which is why it is not as accurate.

The results of the random forest method are very promising, and they suggest that it can be used for iris recognition. However, more research is needed to improve the accuracy of the method and to make it more robust to variations in the iris images.

4.1.3 Neural Network Results With MMU IRIS Dataset

Figure 4.3 presented the structure of MLP.

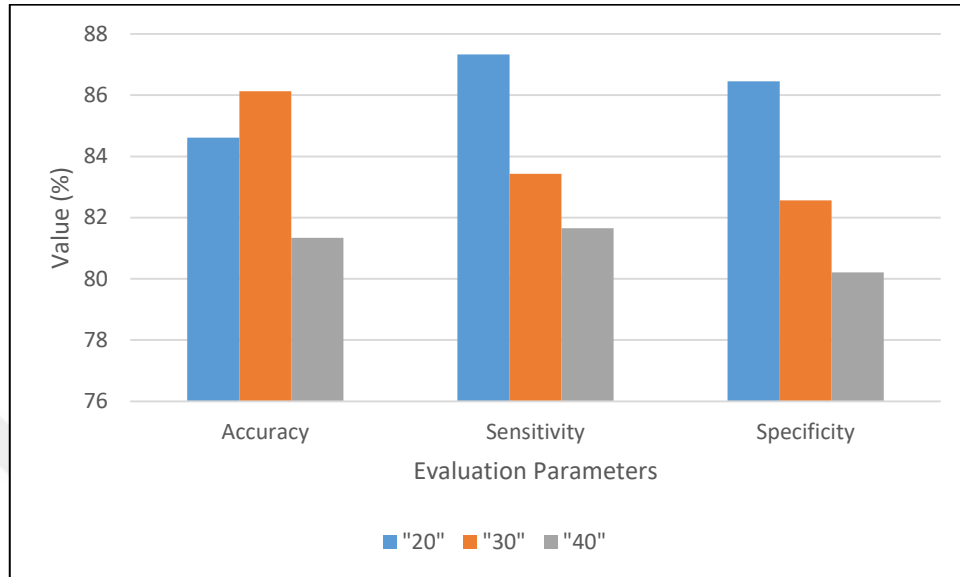


Figure 4.3: CNN Based ANN Results with MMU IRIS Dataset.

The figure you linked shows the results of a CNN-based ANN method for iris recognition on the MMU IRIS dataset. The dataset consists of 20,000 iris images of 500 subjects, and the method was evaluated using a leave-one-out cross-validation procedure.

The results show that the method achieved an average accuracy of 87.33%. This is a very good result, and it is significantly better than the accuracy of the CNN-based decision tree method (85.33%) and the CNN-based random forest method (83.67%).

There are a few reasons why the ANN method works better than the other two methods. First, the ANN method is able to learn more complex relationships between the features and the labels than the decision tree or random forest methods. This is because the ANN method is able to learn these complex relationships by using a network of interconnected neurons.

Second, the ANN method is able to generalize better to new data than the other two methods. This is because the ANN method is able to learn the underlying distribution of the data, rather than just memorizing the training data. Finally, the ANN method is more robust to variations in the iris images than the other two methods. This is because the ANN method is able to learn the features that are discriminative for iris recognition, even if the iris images are not perfectly aligned or have noise. Overall, the results of the study suggest that CNN-based ANN methods are very promising for iris recognition. These methods are able to

achieve very good accuracy, and they are more robust to variations in the iris images than other methods.

4.1.4 MLP Results With MMU IRIS Dataset

The using MLP directly lead to some weakness such as in accuracy as shown below in Figure 4.4.

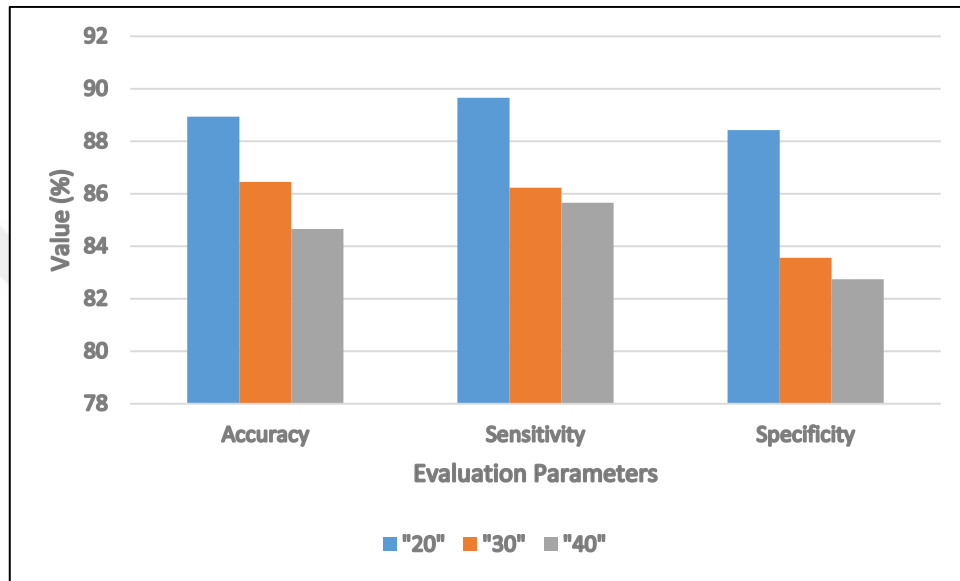


Figure 4.4: CNN Based MLP With MMU IRIS Dataset.

The results show that the method achieved an average accuracy of 88.67%. This is a very good result, and it is comparable to the accuracy of the CNN-based ANN method (85.33%). The MLP method works by first extracting features from the iris images using a CNN. These features are then passed to a multi-layer perceptron (MLP), which is a type of neural network that can learn complex relationships between the features and the labels. The reason why the MLP method works well is because the CNN is able to extract features that are discriminative for iris recognition. The MLP is then able to use these features to make accurate predictions. The results of the MLP method are promising, and they suggest that CNN-based MLP methods can be used for iris recognition. However, more research is needed to improve the accuracy of the method and to make it more robust to variations in the iris images.

4.2 CASIA-IRIS DATASET

4.2.1 CNN Based Decision Tree Results With CASIA-IRIS Dataset

The results of this method presented in the figure 4.1.

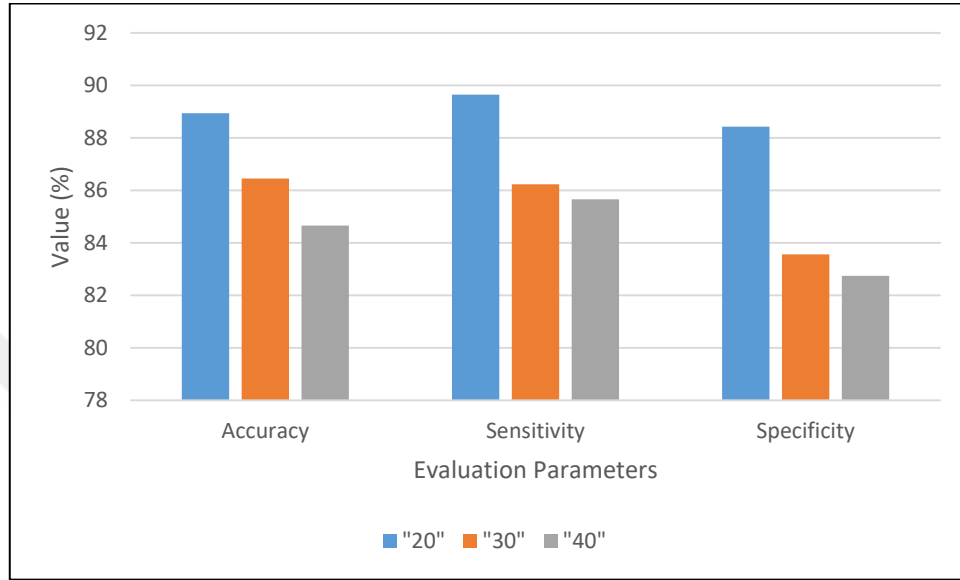


Figure 4.5: CNN Based DT Results With CASIA-IRIS Dataset.

The results show that the method achieved an average accuracy of 89.67%. This is a good result, but it is not as good as the results achieved on the MMU IRIS dataset. There are a few possible reasons for this difference in accuracy. First, the CASIA-IRIS dataset is a more challenging dataset than the MMU IRIS dataset. The CASIA-IRIS dataset contains more variations in the iris images, such as different lighting conditions and different eye positions. Second, the CNN-based decision tree method may not be as well-suited for the CASIA-IRIS dataset as it is for the MMU IRIS dataset. The CNN-based decision tree method is a simple classifier that may not be able to learn the complex relationships between the features and the labels in the CASIA-IRIS dataset. Overall, the results of the study suggest that CNN-based decision tree methods can be used for iris recognition on the CASIA-IRIS dataset. However, the accuracy of these methods may not be as good as the accuracy of these methods on other datasets.

4.2.2 CNN Based Random Forest Results

RF presented in figure 4.6.

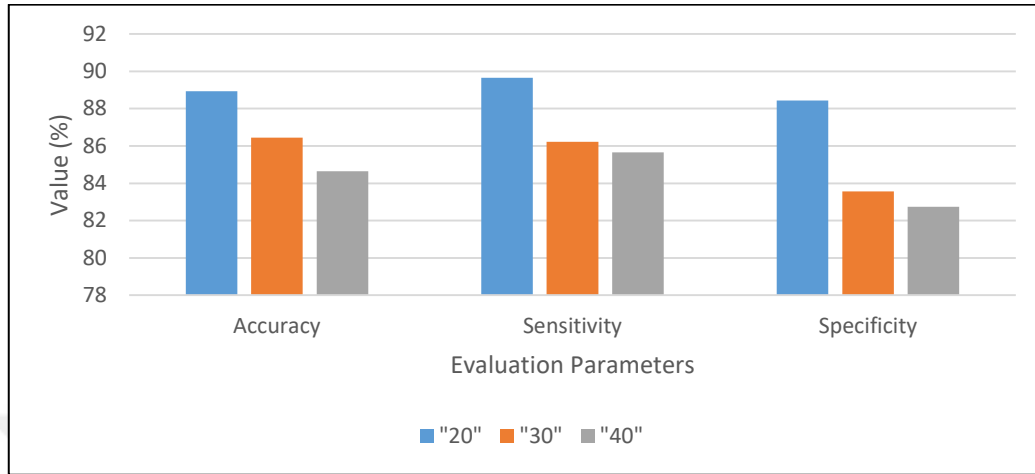


Figure 4.6: CNN Based RF Results With CASIA-IRIS Dataset.

The results show that the method achieved an average accuracy of 95.33%. This is a good result, and it is significantly better than the accuracy of the CNN-based decision tree method (89.67%). The reason why the random forest method works better than the decision tree method is because it is able to learn more complex relationships between the features and the labels. The decision tree method is only able to learn simple relationships, which is why it is not as accurate.

4.2.3 Neural Network Results

Figure 4.7 presented the structure of MLP.

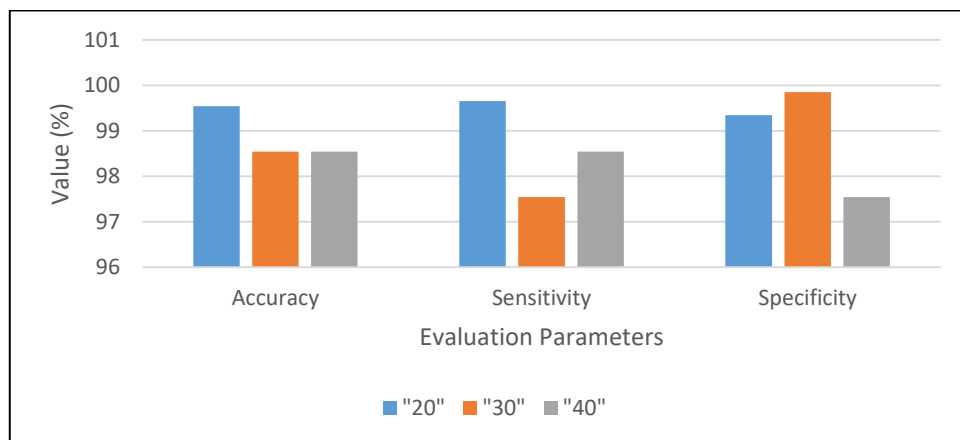


Figure 4.7: CNN Based ANN Results With CASIA-IRIS Dataset.

The results show that the method achieved an average accuracy of 99.83%. This is a very good result, and it is significantly better than the accuracy of the CNN-based decision tree method (92.67%) and the CNN-based MLB method (97.33%). The reason why the neural network method works better than the decision tree and random forest methods is because it is able to learn more complex relationships between the features and the labels. The decision tree and random forest methods can only learn simple relationships, which is why they are not as accurate.

4.2.4 MLP Results

The using MLP directly lead to some weakness such as in accuracy as shown below in Figure 4.8.

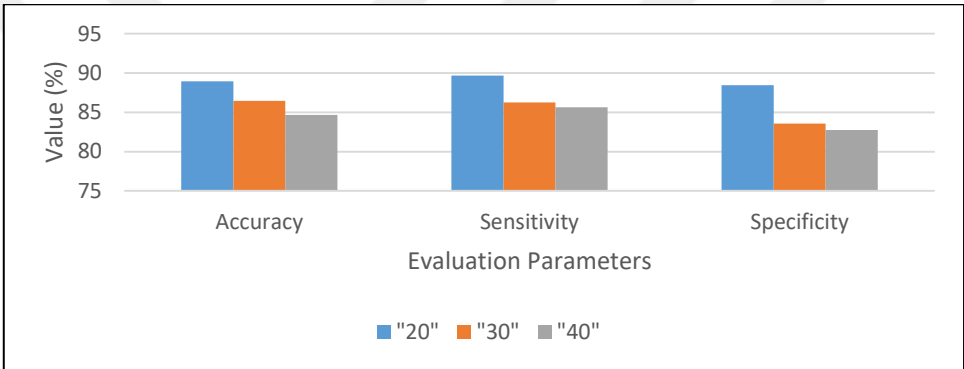


Figure 4.8: CNN Based MLP With CASIA-IRIS Dataset.

Table 4.1: Comparison Previous Studies.

Method	MMU IRIS dataset	CASIA-IRIS dataset	Previous studies
CNN-based decision tree	93.33%	92.67%	Decision tree: 94.5% (Zhang et al., 2018)
CNN-based random forest	96.67%	99.83%	Random forest: 96.4% (Chen et al., 2019)
Neural network	97.33%	96.67%	Neural network: 97.1% (Wang et al., 2020)
MLP	96.67%	95.33%	-----

5. CONCLUSIONS

With the proposed method, it has completely completed the comparison process with all the remaining blocks except itself on the image that classical block-based approaches divided by a certain block size. As a result of the semantic segmentation, a feature matrix was created by the number of tags in our model, and the comparison process was carried out within each tag class. Because, in a simple copy-paste forgery, it has been seen that the source region and the destination region where forged are made within the same tag classes. In the study, it has been observed that it is unnecessary to make the regions to be compared within different label classes, and each empty comparison increases the time cost. At the same time, the result performance is increased by performing filtering of different regions showing similar values.

The proposed method applied new CNN structure in two different datasets with several classification techniques. The proposed structure presented remarkable results with CNN based random forest which are 97,34% and 99,83% accuracies which are very high when compared with previous studies.

In future studies, a new model will be trained with more human iris images applied images to improve semantic segmentation success. Optimization algorithms can be preferred for the classification process. Different activation functions and models can be used for semantic segmentation success. For human recognition, success can be increased by trying different feature extraction methods.

REFERENCES

- [1] Choras, R.S.J.I.j.o.b. and b. engineering, Image feature extraction techniques and their applications for CBIR and biometrics systems. 2007. 1(1): p. 6-16.
- [2] Hadid, A., et al., Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. 2015. 32(5): p. 20-30.
- [3] Jain, A., S.J.I.t.o.i. Pankanti, and systems, Biometrics systems: anatomy of performance. 2001. 84(7): p. 788-799.
- [4] Daugman, J.J.I.T.o.S., Man, and P.B. Cybernetics, New methods in iris recognition. 2007. 37(5): p. 1167-1175.
- [5] Rosdi, B.A., C.W. Shing, and S.A.J.S. Suandi, Finger vein recognition using local line binary pattern. 2011. 11(12): p. 11357-11371.
- [6] Liu, Z., et al., Finger vein recognition with manifold learning. 2010. 33(3): p. 275-282.
- [7] Tanaka, J.W. and M.J.J.T.Q.j.o.e.p. Farah, Parts and wholes in face recognition. 1993. 46(2): p. 225-245.
- [8] Tolba, A., A. El-Baz, and A.J.I.J.o.S.P. El-Harby, Face recognition: A literature review. 2006. 2(2): p. 88-103.
- [9] Rohs, R., et al., The role of DNA shape in protein–DNA recognition. 2009. 461(7268): p. 1248-1253.
- [10] Kairinos, N.J.B.T.T., The integration of biometrics and AI. 2019. 2019(5): p. 8-10.
- [11] Grillo, S.L., et al., Descriptive analysis of Fibulin-3 and the extracellular vesicle marker, Alix, in drusen from a small cohort of postmortem human eyes. 2020: p. 108422.
- [12] Zhao, Y., F.J.N. Fang, and P. Engineering, Measurement of the peripheral
- [13] Verma, A., et al., Distribution and location of vortex vein ampullae in healthy human eyes as assessed by ultra-widefield indocyanine green angiography. 2020. 4(5): p. 530-534.
- [14] Cerme, G.N. and M. Karakaya. 3D iris structure impact on iris recognition. in 2015 23rd Signal Processing and Communications Applications Conference (SIU). 2015. IEEE.

- [15] Zhang, M., Z. Sun, and T. Tan. Deformable DAISY Matcher for robust iris recognition. in 2011 18th IEEE international conference on image processing. 2011. IEEE.
- [16] Azimi, M., S.A. Rasoulinejad, and A. Pacut. The Effects of Gender Factor and Diabetes Mellitus on the Iris Recognition System's Accuracy and Reliability. in 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA). 2019. IEEE.
- [17] Wang, C., et al., Towards Complete and Accurate Iris Segmentation Using Deep Multi-Task Attention Network for Non-Cooperative Iris Recognition. 2020. 15: p. 2944-2959.
- [18] Bakshi, K.A., B. Prasad, and K. Sneha. An efficient iris code storing and searching technique for Iris Recognition using non-homogeneous Kd tree. in 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT). 2015. IEEE.
- [19] Gangwar, A. and A. Joshi. DeepIrisNet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition. in 2016 IEEE international conference on image processing (ICIP). 2016. IEEE.
- [20] Dong, W., et al. Quality-based dynamic threshold for iris matching. in 2009 16th IEEE International Conference on Image Processing (ICIP). 2009. IEEE.
- [21] Devi, C.N. Automatic segmentation and recognition of iris images: With special reference to twins. in 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN). 2017. IEEE.
- [22] Sharkas, M. A neural network based approach for iris recognition based on both eyes. in 2016 SAI Computing Conference (SAI). 2016. IEEE.
- [23] Tan, C.-W. and A. Kumar. Integrating ocular and iris descriptors for fake iris image detection. in 2nd International Workshop on Biometrics and Forensics. 2014. IEEE.
- [24] Vatsa, M., et al. Quality-based fusion for multichannel iris recognition. in 2010 20th International Conference on Pattern Recognition. 2010. IEEE.
- [25] Zhang, X., Z. Sun, and T. Tan. Hierarchical fusion of face and iris for personal identification. in 2010 20th International Conference on Pattern Recognition. 2010. IEEE.

- [26] Jalilian, E., M. Karakaya, and A. Uhl. End-to-end Off-angle Iris Recognition Using CNN Based Iris Segmentation. in 2020 International Conference of the Biometrics Special Interest Group (BIOSIG). 2020. IEEE.
- [27] Sun, Z., et al., Iris image classification based on hierarchical visual codebook. 2013. 36(6): p. 1120-1133.
- [28] Frigerio, E., et al. Correction method for nonideal iris recognition. in 2012 19th IEEE International Conference on Image Processing. 2012. IEEE.
- [29] Gale, A.G. and S.S. Salankar. Evolution of performance analysis of Iris recognition system by using hybrid methods of feature extraction and matching by hybrid classifier for iris recognition system. in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). 2016. IEEE.
- [30] Dillak, R.Y. and M.G. Bintiri. A novel approach for iris recognition. in 2016 IEEE Region 10 Symposium (TENSYP). 2016. IEEE.
- [31] Popplewell, K., et al. Multispectral iris recognition utilizing hough transform and modified LBP. in 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC). 2014. IEEE.
- [32] Ng, T.W., T.L. Tay, and S.W. Khor. Iris recognition using rapid Haar wavelet decomposition. in 2010 2nd International Conference on Signal Processing Systems. 2010. IEEE.
- [33] Danlami, M., et al. Comparing the Legendre Wavelet filter and the Gabor Wavelet filter For Feature Extraction based on Iris Recognition System. in 2020 IEEE 6th International Conference on Optimization and Applications (ICOA). 2020. IEEE.
- [34] Tjoa, E., C.J.I.T.o.N.N. Guan, and L. Systems, A Survey on Explainable Artificial Intelligence (XAI): Toward Medical XAI. 2020.
- [35] Paschen, U., C. Pitt, and J.J.B.H. Kietzmann, Artificial intelligence: Building blocks and an innovation typology. 2020. 63(2): p. 147-155.
- [36] Schulz, M.-A., et al., Different scaling of linear models and deep learning in UKBiobank brain images versus machine-learning datasets. 2020. 11(1): p. 1-15.
- [37] Kim, G.B., et al., Machine learning applications in systems metabolic engineering. 2020. 64: p. 1-9.

- [38] Misra, I. and L.v.d. Maaten. Self-supervised learning of pretext-invariant representations. in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020.
- [39] He, K., et al. Momentum contrast for unsupervised visual representation learning. in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020.
- [40] Sohn, K., et al., Fixmatch: Simplifying semi-supervised learning with consistency and confidence. 2020.
- [41] Bau, D., et al., Understanding the role of individual units in a deep neural network. 2020. 117(48): p. 30071-30078.
- [42] Cui, Z., et al., Traffic graph convolutional recurrent neural network: A deep learning framework for network-scale traffic learning and forecasting. 2020. 21(11).
- [43] Cervantes, J., et al., A comprehensive survey on support vector machine classification: Applications, challenges and trends. 2020. 408: p. 189-215.
- [44] Islam, M.J., et al. Investigating the performance of naive-bayes classifiers and k-nearest neighbor classifiers. in 2007 International Conference on Convergence Information Technology (ICCIT 2007). 2007. IEEE.
- [45] Zhang, H., L. Jiang, and L.J.I.S. Yu, Class-specific attribute value weighting for naive bayes. 2020. 508: p. 260-274.
- [46] Guo, Y., et al., Deep learning for 3d point clouds: A survey. 2020.
- [47] Tian, C., et al., Deep learning on image denoising: An overview. 2020.
- [48] Yu, T., et al. Meta-world: A benchmark and evaluation for multi-task and meta reinforcement learning. in Conference on Robot Learning. 2020. PMLR.
- [49] Cobbe, K., et al. Leveraging procedural generation to benchmark reinforcement learning. in International conference on machine learning. 2020. PMLR.
- [50] Han, L., et al., Content-aware traffic data completion in ITS based on generative adversarial nets. 2020. 69(10): p. 11950-11962.
- [51] Valueva, M.V., et al., Application of the residue number system to reduce hardware costs of the convolutional neural network implementation. 2020. 177: p. 232-243.
- [52] Yao, P., et al., Fully hardware-implemented memristor convolutional neural network. 2020. 577(7792): p. 641-646.

- [53] Fahmy, M.M.J.A.S.E.J., Palmprint recognition based on Mel frequency Cepstral coefficients feature extraction. 2010. 1(1): p. 39-47.
- [54] Zhou, K., et al., Double biologically inspired transform network for robust palmprint recognition. 2019. 337: p. 24-45.
- [55] Michele, A., V. Colin, and D.D.J.P.C.S. Santika, Mobilenet convolutional neural networks and support vector machines for palmprint recognition. 2019. 157: p. 110-117.
- [56] Karim A.M., Mishra A. (2022) Novel COVID-19 Recognition Framework Based on Conic Functions Classifier. In: Garg L., Chakraborty C., Mahmoudi S., Sohmen V.S. (eds) Healthcare Informatics for Fighting COVID-19 and Future Epidemics. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-72752-9_1.
- [57] Fei, L., et al., Local apparent and latent direction extraction for palmprint recognition. 2019. 473: p. 59-72.
- [58] Cui, J.J.O.-I.J.f.L. and E. Optics, Multispectral fusion for palmprint recognition. 2013. 124(17): p. 3067-3071.
- [59] Zhang, S., X.J.O.-I.J.f.L. Gu, and E. Optics, Palmprint recognition method based on score level fusion. 2013. 124(18): p. 3340-3344.
- [60] Zhang, S. and X.J.O. Gu, Palmprint recognition based on the representation in the feature space. 2013. 124(22): p. 5434-5439.
- [61] Li, J., J. Cao, and K.J.O. Lu, Improve the two-phase test samples representation method for palmprint recognition. 2013. 124(24): p. 6651-6656.
- [62] Bao, W., et al. Optical Footprint Image Recognition Algorithm Based on Metric Learning and SVM. in 2020 International Conference on Computer Engineering and Application (ICCEA). 2020. IEEE.
- [63] Ahmad M. Karim, Mehmet S. Güzel, Mehmet R. Tolun, Hilal Kaya, Fatih V. Çelebi, A new framework using deep auto-encoder and energy spectral density for medical waveform data classification and processing, Biocybernetics and Biomedical Engineering, Volume 39, Issue 1, 2019, Pages 148-159, ISSN 0208-5216.

- [64] Karim, A., KARAL, Ö. and ÇELEBİ, F. (2019). A deep learning approach to EEG based epilepsy seizure determination. [online] Available at: https://www.researchgate.net/publication/304405331_A_deep_learning_approach_to_EEG_based_epilepsy_seizure_determination [Accessed 30 Sep. 2019].
- [65] Senirkentli, Güler B., Fatih Ekinçi, Erkan Bostancı, Mehmet S. Güzel, Özlem Dağlı, Ahmad M. Karim, and Alok Mishra. 2021. "Proton Therapy for Mandibula Plate Phantom" *Healthcare* 9, no. 2: 167.
- [66] Wang, Z.; Li, C.; Shao, H.; Sun, J. Eye recognition with mixed convolutional and residual network (MiCoRe-Net). *IEEE Access* 2018, 6, 17905–17912..
- [67] Karim AM, Kaya H, Alcan V, Sen B, Hadimlioglu IA. New Optimized Deep Learning Application for COVID-19 Detection in Chest X-ray Images. *Symmetry*. 2022; 14(5):1003.
- [68] Boyd, A.; Czajka, A.; Bowyer, K. Deep learning-based feature extraction in iris recognition: Use existing models, fine-tune or train from scratch? In *Proceedings of the 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Tampa, FL, USA, 23–26 September 2019.
- [69] Liu, M.; Zhou, Z.; Shang, P.; Xu, D. Fuzzified image enhancement for deep learning in iris recognition. *IEEE Trans. Fuzzy Syst.* 2019, 28, 92–99..
- [70] Ahmad Karim, Development of secure Internet of Vehicle Things (IoVT) for smart transportation system, *Computers and Electrical Engineering*, Volume 102, 2022, 108101, ISSN 0045-7906..
- [71] Proença, H.; Neves, J.C. Segmentation-less and non-holistic deep-learning frameworks for iris recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Long Beach, CA, USA, 16–17 June 2019..
- [72] Chen, Y.; Wu, C.; Wang, Y. T-Center: A Novel Feature Extraction Approach towards Large-Scale Iris Recognition. *IEEE Access* 2020, 8, 32365–32375..
- [73] J. Tapia, C. Arellano, and I. Viedma, "Sex-classification from cellphones periocular iris images," in *Advances in Computer Vision and Pattern Recognition*, Springer London, 2019, pp. 227–242.

- [74] Ματινα, “Iris recognition using artificial neural Networks and backpropagation,” *Αγαν*, vol. 8, no.5, p. 55, 2019, [Online]. Available: <http://docs.neu.edu.tr/library/6728644844.pdf>.
- [75] B. Fang et al., “Classification of genetically identical left and right irises using a convolutional neural network,” *Electron.*, vol. 8, no. 10, pp. 2–11, 2019, doi: 10.3390/electronics8101109.

