Different Biometrical Features for Detecting Human Intrusion Using Artificial Intelligence: Literature Review

Ansam Nazar Younis

University of Mosul, Mosul

*Corresponding author. Email: anyma8@uomosul.edu.iq

Abstract

Abstract—Many cases of theft and property trespass in addition to crimes occur in the world after these people break into people's homes and buildings illegally, so this article aims to shed light on most of the smart methods and computer technologies used in identifying people that help to reduce these crimes. Where the diversity of biometric traits was relied upon, such as fingerprint, handprint, ear, face, texture, some deformations characteristic of people, eye, footprints, DNA analysis and other important biometric traits. Also, many intelligent algorithms were used to identify these traits.

Keywords:
Biometrical features, Practical swarm intelligent, Neural Network.

I. INTRODUCTION

Many smart technologies have been used since the inception of artificial intelligence of all kinds to detect people, whether for security, economic, educational and other purposes. Perhaps one of the most important reasons for using these technologies is their ability to access the required person’s data accurately and in record time. The increase in the crime rate along with the increase in the emergence of many smart and modern technologies has contributed to the use in many countries of these wonderful techniques in detecting criminals who are trying to break into a place or trying to commit any crime. Many technologies are now used for this purpose, including intelligent technologies such as post-intuitive algorithms and modern classification and discrimination algorithms based on identifying the person by some traces that the criminal leaves behind, such as fingerprints, footprints, palm prints, a picture of the face or part of it, the weight of the person, And other well-known biometric features [58].

This review aims to identify the most recently used smart methods in the process of identifying, accessing and detecting criminals and intruders who is trying to intrude on public or private property. We will discuss the Biometric technologies: Human Iris, Face, Palm Vein, Human Retina, Fingerprint, Ear, Signature, Gait Recognition, Acoustic and visual features, Hand Geometry, Voice, Teeth, Skin texture, Footprint, DNA biometric, and Additional biometrical information.

II. BIOMETRICAL FEATURES

1. Human Iris

There are many smart applications that have been developed to reach a high level of protection and security scrutiny, in which the iris was used, as it is considered one of the most biometric properties, which provides distinct and clear physical properties for distinguishing between people, as well as because most intruders hide the greater part of their faces while keeping an area The eyes are exposed. Especially if accurate cameras and high intelligence and software capabilities are used to distinguish and capture a picture of the iris of the human eye quickly enough and then use modern smart algorithms to reach the owner of that iris, but if we
decide to use this method to protect from intruders and reduce crimes, we must realize exactly where we place these cameras to ensure that the person gets close enough to them and without arousing suspicion.

(Fadi N. Sibai) and others They proposed a way to distinguish between people and identify a person by designing a system to recognize the iris of a Feed-forward artificial neural network algorithm [7], genetics [61], and artificial neural network for this purpose [44][62][73]. Here in table 1 some of these properties of last five years.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Dataset</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[73]</td>
<td>JluIrisV3.1, JluIrisV4, and CASIA-V4 Lamp</td>
<td>60,822 class</td>
<td>capsule network,</td>
<td>53.73%, 99.37%</td>
</tr>
</tbody>
</table>

2. Face

Sometimes the intruder is revealing his face or covered with a light sock that modern and smart devices can recognize after making a set of improvements and applying some image clarification algorithms and retrieval of the original images in a way that can distinguish that person and with some smart algorithms, we can identify the intruder’s personality easily and very quickly. Other researchers were able to use the biometric facial feature in order to identify people, know their age, as well as their gender, or just to recognize the faces, using a small training set that is inserted into Posteriori Class probability with or just using artificial neural networks algorithm [8],[30][38]. Deep learning algorithms can also be adopted in home-monitoring devices, buildings and various institutions, as the researchers suggested (Van-Huy Pham, Diem-Phuc Tran, and Van-Dung Hoang) using deep learning algorithms to identify and distinguish different people based on images of human faces taken by traditional cameras of low quality and accuracy [3]. The researchers Saroj Bijarnia and Preety Singh also used some facial features less changing with age to identify people using Support vector machine algorithm [15]. The researchers also used the geometric measurements of the face, such as the distance between the pupil of the right and the pupil of the left, as inputs to conditional mutual information with nearest neighbor’s estimate (CMIUN) [19]. While the researcher Thai Hoang Le proposed a hybrid intelligent method that combines two algorithms (AdaBoost, Artificial Neural Network) to distinguish faces after determining the geometric features of the face alignment [23]. While other researchers used the method of determining other geometric features of the human face, such as the locations of the eyebrows, eyes, the location of the nose, mouth, ears, and others, with the intelligent algorithm (Radial Basis Function (RBF)), which is one of the types of neural networks [25][63][65]. The researchers (Kolhandai Yesu and others) also relied on the geometric measurements of the face, eyes, nose and mouth as inputs to the intelligent feed-forward neural network [32].

In another research [51], the face, eyes, mouth and nose were used to identify people using the intelligent cuckoo search algorithm, Fig. (1)

![Figure 1. Identify people through face, eyes, nose, mouth features](image)

Here in table 2 some of these properties of last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Dataset</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[65]</td>
<td>Nvidia RTX 2070</td>
<td>150</td>
<td>deep neural network</td>
<td>77.82%</td>
</tr>
</tbody>
</table>

3. Palm Vein

The researchers (Mona A. Ahmed, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Sale) provided the use of one of the most important physiological characteristics in identifying people with high reliability, which is the palm vein. These veins were identified in the palm after processing images that were taken by the CASIA device (V1.0 (CASIA) of the hand and then identified by an algorithm(k-Nearest Neighbors (KNN) classifier)[1], also Sarah Hachemi Benziane and Abdelkader Benyettou, suggested identification system for the same biometrical features by using practical swarm intelligent algorithm[37], in [6] the researcher uses ANN(artificial neural network) with Gaussian filter for the same purpose, also in[64] proposed dorsal hand vein using Convolutional Neural Network (CNN). Here in table 3 some of these papers of last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[37]</td>
<td>NCUT database</td>
<td>2040</td>
<td>Binary Particle Swarm Optimization</td>
<td>100%</td>
</tr>
<tr>
<td>[6]</td>
<td>Live dataset</td>
<td>100</td>
<td>Artificial Neural Network</td>
<td>92%</td>
</tr>
</tbody>
</table>

4. Human Retina

For Dr. (I. Jeena Jacob), he suggested using the human retina features as one of the most important types of biological features known to identify people and using the capsule neural network these features were distinguished [4]. On the same curriculum, the researchers (Khattab M. Ali Alheeti and others) used the same intelligent method with the addition of fuzzy logic [17]. Also, in [59] the researchers supposed a
method for detect the diseases in retina which can be used in human detection. In table 4 some of these properties of papers in the last five years:

**TABLE (4) PROPERTIES OF HUMAN RETINA PAPERS**

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[4]</td>
<td>CASIA-Iris</td>
<td>1000</td>
<td>CAPSULE NETWORK</td>
<td>99%</td>
</tr>
<tr>
<td>[17]</td>
<td>DRIVE dataset</td>
<td>200 neurons input</td>
<td>Fuzzification Neural Network</td>
<td>98.20%</td>
</tr>
<tr>
<td>[59]</td>
<td>SD-OCT data-set</td>
<td>1000</td>
<td>CNN</td>
<td>98.8%, 100%</td>
</tr>
</tbody>
</table>

5. Fingerprint

To achieve a high percentage of security, the researchers (Asker M. Bazen and Sabih H. Gerez) used the fingerprint pattern with the application of intelligence algorithms to identify people's fingerprints. Genetic programming was used in the factors for exploring fingerprint images, thus obtaining a more reliable recognition system that obtains the important characteristics from the images of those fingerprints, which are considered One of the easiest images that can be obtained from hacker intrusion sites [5]. While in [67], [74] the researchers used NN. In table 5 some of these paper for last five years:

**TABLE 5. PROPERTIES OF HUMAN FINGERPRINT PAPERS**

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[67]</td>
<td>A live dataset</td>
<td>25</td>
<td>ANN</td>
<td>100%</td>
</tr>
<tr>
<td>[74]</td>
<td>PolyU</td>
<td>1480</td>
<td>CNN</td>
<td>95.7%</td>
</tr>
</tbody>
</table>

6. Ear Biometric

The human ear may be considered one of the most important vital characteristics in identifying intruders, especially in public places that need more protection and security. The identity of people may be checked and examined by the human ear and the identification of criminals without the knowledge of the person who was subjected to security scrutiny, especially during the day or in places Illuminated for the ease of capturing images of the ear by cameras even far from the person for a sufficient distance. Also, the human ear does not change over time and is not exposed to camouflage or concealment, such as the eyes, face or teeth, with the ability to reach a high percentage of biometric recognition rates in the different systems. In [46] researcher use this biometry with neural network for this purpose, while (Asmaa Sabet Anwara, Kareem Kamal A. Ghanyb, Hesham Elmahdy) used a method to identify people through the image of the human ear in order to facilitate obtaining an image of the ear through cameras, it is visible and clear to the lenses. After processing the image, multiple treatments are distinguished from each other using (nearest neighbour) [2], while CNN used in [75], and [76] table 6 paper for last five years:

**TABLE 6. PROPERTIES OF HUMAN EAR PAPERS**

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[75]</td>
<td>USTB</td>
<td>79</td>
<td>CNN</td>
<td>97.9%</td>
</tr>
<tr>
<td>[76]</td>
<td>A live dataset</td>
<td>250</td>
<td>CNN</td>
<td>90%, 95%</td>
</tr>
</tbody>
</table>

7. Signature

It may be difficult to obtain the signature of a criminal who is trying to penetrate homes and other buildings, but there are some cases that make a professional criminal able to forge some papers to obtain money and other property by imitating the signature of the people who are the real owners of that money. Accurate using algorithms and intelligent systems.

Using extracted features, morphological properties, and a Feed Forward Neural Network algorithm, (Vibha Pandey, Sanjivani Shantaiya) researchers have proposed a system for distinguishing people through off-line signature recognition on paper [9]. In [16] and [29] also neural networks were used for the same purpose. Also, in [20] and [45] the researchers used an artificial neural network (ANN) to classify a person's signature using geometric features. Also, the verification of digital signatures by structural and statistical features can contribute to the process of verifying the personality after its introduction to the artificial neural network. This technique was used by researchers H. Said-Ahmed and E. Natsheh [22]. While the two researchers (M. Taylan DÜLGER) used the hybrid particle swarm algorithm with the neural network for the same purpose [24], as for [66] design a recognition system using NN, In table 7 some of these paper for last five years:

**TABLE 7. PROPERTIES OF HUMAN SIGNATURE PAPERS**

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[20]</td>
<td>MCYT, BHSig260</td>
<td>100</td>
<td>ANN</td>
<td>83%_97%</td>
</tr>
<tr>
<td>[45]</td>
<td>SigComp</td>
<td>&gt;230</td>
<td>ANN</td>
<td>80%_100%</td>
</tr>
<tr>
<td>[22]</td>
<td>A live data</td>
<td>20</td>
<td>ANN</td>
<td>75%</td>
</tr>
<tr>
<td>[24]</td>
<td>data acquisition</td>
<td>100</td>
<td>PSO-NN</td>
<td>75%</td>
</tr>
</tbody>
</table>

8. Gait Recognition

In 2013 Gibin Thomas and Kapil Nagwanshi suggested a method for detecting a person's gait deformity, through which the type of foot is identified, whether it is flat or not using Artificial Neural Network (ANN). This feature, if discovered, may help determine some of the characteristics of the intruder [10]. The researchers also followed Shahlla A. AbdAlKader and Omaima N. Ahmad AL-Allaf the same method, but by using the particle swarm optimization algorithm to identify people by the way they walked[14].

The researcher Sruthy Sebastian showed an improved way to distinguish people by recognizing objects and the person's movement from several angles and with several different movements using the particle swarm algorithm with linear
discrimination analysis. Cameras are unable to capture the basic features of other types of biometric features; the particle swarm algorithm was used in the discrimination process [26]. Continuous monitoring devices can be used to detect pedestrians by using different gaming networks. The researchers, Wei Li and others, used FPNN: filter pairing neural network algorithm to implement this idea [31], in [72] used ENN with NN for the same purpose. Table 8 for last five years of research:

TABLE 8. PROPERTIES OF HUMAN GAIT RECOGNITION PAPERS

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[26]</td>
<td>A live dataset</td>
<td>Multi period of movie</td>
<td>particle swarm optimization (PSO)</td>
<td>94.37%</td>
</tr>
</tbody>
</table>

9. Acoustic and visual features

As for the audio and visual qualities, they can be used to identify the intruder on the place, like saying certain words, using custom language, or wearing some special, as suggested by the researchers Roberto Brunelli and Daniele Falavigna. For this purpose, HyperBF networks were used [11]. Also, in paper [48], the ant lion algorithm was used for this purpose. We may be able to identify the intruder who does not use masks or methods of disguise, such as terrorists, and these enter among ordinary people and pretend that they are ordinary people, by identifying some of the facial expressions that appear on their faces against their will, so we can resort to artificial intelligence to solve this problem, Wesam A. A. Asker distinguished some expressions such as , fear, disgust ,anger, joy, surprise, sadness using the neural network[36]. Note table 9 for some of these paper in last five years:

TABLE 9. PROPERTIES OF ACOUSTIC AND VISUAL FEATURES PAPERS

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of samples</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[48]</td>
<td>A live dataset</td>
<td>1800</td>
<td>Ant Lion Algorithm</td>
<td>99%</td>
</tr>
</tbody>
</table>

10. Hand Geometry

In many smart methods, the geometric measurements of the human hand have been relied upon to collect information about people and identify them. One of these methods is to use that information as input parameters to the convolutional neural network in a back-propagation method. This idea was implemented by many researchers [12][42]. Many authors use the same method, but by taking the measurements of the four fingers only and identifying the owner using Artificial Neural Network (ANN) and distance based nearest neighbor (DBNN) algorithms [39][41], and [68] which is used BPNN: backpropagation NN. Note table 10 for some of these paper in last five years:

TABLE 10. PROPERTIES OF HUMAN HAND GEOMETRY PAPERS

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of samples</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[42]</td>
<td>A live dataset</td>
<td>100</td>
<td>back propagation NN</td>
<td>88%_.95%</td>
</tr>
<tr>
<td>[68]</td>
<td>A live dataset</td>
<td>100</td>
<td>BPNN</td>
<td>93%</td>
</tr>
</tbody>
</table>

11. Voice

Arsha Nagrani and others [18], and Viresh Moonasar Ganesh K. Venayagamoorthy [28] researchers proposed a way to use convolutional neural networks in the process of identifying a the tone of voice, in [69] Lubna and others using fuzzy logic with neural network for Arabic voice recognition, also in [48] research the authors used Arabic voice people for recognized the Arabic numbers which can be used for recognized the people themselves, Table 11 for some paper in the last five years:

TABLE 11. PROPERTIES OF HUMAN VOICE PAPERS

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of samples</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[18]</td>
<td>VoxCeleb</td>
<td>100,000</td>
<td>CNN</td>
<td>92.1%</td>
</tr>
<tr>
<td>[69]</td>
<td>A live dataset</td>
<td>250</td>
<td>Fuzzy Logic and Neural Network</td>
<td>94%</td>
</tr>
<tr>
<td>[48]</td>
<td>A live dataset</td>
<td>1800</td>
<td>Ant Lion Algorithm</td>
<td>99%</td>
</tr>
</tbody>
</table>

12. Teeth Biometric

The intruder may use some camouflage and distortion of his outer shape, and at the same time, the shape of his teeth remains in the case of smiling or opening the mouth to speak clearly in front of the camera. For this, some researchers have suggested a way to identify people after taking pictures of the person’s teeth and mouth using an artificial neural network and this is what was done in the research [21]. It is possible to use other methods in criminal reports, for example, determining the age of the intruder by measuring the gradual development of the teeth and using multiple intelligent algorithms, and this is done if the intruder is injured so that the teeth or his body are available [43]. In addition, x-rays can be used to identify people in the event of finding unidentified persons using a database that maintains information on x-rays of the jaw, face and skull, using particle swarm optimization, and contourlet PSO as in the two research [47][49]. Note table 12 for paper in the last five years:

TABLE 12. PROPERTIES OF HUMAN TEETH BIOMETRIC PAPERS

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of samples</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[21]</td>
<td>A live dataset</td>
<td>10 pictures for each person</td>
<td>ANN</td>
<td>81.69%</td>
</tr>
<tr>
<td>[43]</td>
<td>Kovai</td>
<td>100</td>
<td>ENN</td>
<td>72% 92.3%</td>
</tr>
<tr>
<td>[47]</td>
<td>A live dataset</td>
<td>125</td>
<td>PSO</td>
<td>98%</td>
</tr>
<tr>
<td>[49]</td>
<td>A live dataset</td>
<td>100</td>
<td>Contourlet PSO</td>
<td>98%</td>
</tr>
</tbody>
</table>
13. Skin Texture

Regarding this biometric feature, it is considered very important because intruders often use door handles and touch things and then scan the place of their fingerprints. The tactile sensor can be used as a new technology that can be added to the places that the intruder can use and touch as the system identifies person who touches this piece Skin directly by examining the texture. (Toshinobu and others) worked on developing this idea based on the intelligent particle swarm algorithm [27], in [13] Idoko John Bush and others used Neuro Fuzzy Inference System to detect the skin color of person, as for [70] feed forward neural networks algorithm is used for same purpose. Table 13 is the paper properties for last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[27]</td>
<td>A live dataset</td>
<td>70</td>
<td>Soft Robotics</td>
<td>90%</td>
</tr>
<tr>
<td>[13]</td>
<td>A live dataset</td>
<td>100</td>
<td>Fuzzy</td>
<td>89% 90.10%</td>
</tr>
</tbody>
</table>

14. Footprint

In many cases of theft and unwanted intrusion around the world, the intruder is barefoot, and for this reason, images of the foot can be used in the process of identifying the intruder, and this is what the researchers reached in the two research [53][54] using smart neural networks, while in [71] Recognition Footprint Characteristics for of the baby by using K-Nearest Neighbor (K-NN). Table 14 is the paper properties for last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[71]</td>
<td>A live dataset</td>
<td>180</td>
<td>KNN</td>
<td>99.30%</td>
</tr>
</tbody>
</table>

15. DNA Biometric

Perhaps the DNA analysis is one of the most important biometric characteristics because the aggressor may lose a hair during the robbery or intrusion process, or it may be a crime of rape, leaving other traces useful in this area. Therefore, many developers turned to developing systems based on the analysis of the DNA mainly in identifying strangers. The researchers (Laheeb M. Alzoubiady, Ibrahim A. Saleh) tended to design a personal identification system that relies on more than one biometric characteristic, the most important of which is the characteristics of the DNA and used for this purpose the particle swarm algorithm [34]. also, in [56][77] the authors use neural network for the same purpose. Table 15 is the paper properties for last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[77]</td>
<td>MPRA</td>
<td>500,000</td>
<td>CNN</td>
<td>High_quality</td>
</tr>
</tbody>
</table>

16. Additional biometrical information

We may sometimes resort to some secondary biometric traits to reach people easily by adding the original traits of the person, as the more information about the required person, the better the assurance of the intruder’s personality. For example, in [33] research, the researchers (Zayd Assyafir Alaydrus1 and others) suggested a way to determine whether a person has diabetes or not by analyzing the image of the retina and using the intelligent neural network for this purpose. Also, Fatin Atiqah Rosli and others use multi-intelligence techniques such that k-Nearest Neighborhood (k-NN) and Support Vector Machine (SVM) and MLP, for recognize the person is tuberculosis or not, using samples of sputum or saliva of the patient [40], or by detecting a tumor or disease in the eye by Fuzzy system, as in [52]. It is also possible to discover some skin diseases in the intruder, which may help to identify him, as in the research [50], where several smart techniques were used, some types of body cancers can also be identified by taking a blood biopsy, such as detecting lung cancer using ANN as for [55]. Table 16 is the paper properties for last five years:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Source of the biometric images</th>
<th>Number of images</th>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[33]</td>
<td>STARE</td>
<td>248</td>
<td>ANN</td>
<td>96.67%</td>
</tr>
<tr>
<td>[40]</td>
<td>ZN-stained</td>
<td>70</td>
<td>SVM</td>
<td>94.1%</td>
</tr>
<tr>
<td>[50]</td>
<td>kaggle</td>
<td>2000</td>
<td>multi-intelligent techniques</td>
<td>79%_100%</td>
</tr>
<tr>
<td>[55]</td>
<td>lungca</td>
<td>675</td>
<td>ANN</td>
<td>100%</td>
</tr>
</tbody>
</table>

III. STANDARDS USED TO COMPARE BIOMETRIC TRAITS

We have used some standards and laws that help us reach the most important biometric characteristics that can be relied upon in the security systems of personal homes, government buildings, malls and important civil buildings. Among those criteria are the following: Through our follow-up to a lot of research and sources, we found that some of the standards used in comparing those attributes that are:

1. Performance: This feature shows how efficient the biometric feature is in identifying people.
2. Permanence: This feature shows the continuity of the biometric characteristic over different time periods.
3. Universality: The trait must be possessed by everyone. It must be a universal feature that is rarely lost due to accident or disease.
4. Uniqueness: can be defined through secondary matters of human biometric characteristics, for example, in the case of a fingerprint, there is a very low probability of repeating the same fingerprint in more than one person while other characteristics are similar, it is possible with the same feature in different proportions between more than one person, such as tone of voice, hand measurements, and others.

5. Acceptance: Capturing should be possible in a way that is acceptable to a significant portion of the population. Particularly persistent technologies, such as those that necessitate the taken of a component of the human body or that (seemingly) harm the human body, are excluded.

6. Collectability: This feature means the possibility of obtaining data and the ability to collect it easily or not.

7. Circumvention: This trait describes the extent to which the biometric trait can detect a character in an intelligent or in elusive manner.

8. Ease of use: This feature can be defined from several aspects, including the availability of the required devices, which affects the ease of use, as well as the behavior of the intruder towards monitoring devices.

9. Accuracy: This feature discusses the accuracy of identifying different people if the biometric feature is used. By following up on a lot of research and references, it was concluded that these criteria are important in deciding the type of biometric characteristic that is desired. These results can be observed through table (17) and table (18) of comparisons between those criteria for all the proposed biometric characteristics:

**TABLE 17. COMPARISON OF SUM BIOMETRIC TRAITS**

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Collectability</th>
<th>Circumvention</th>
<th>Ease Of Use</th>
<th>Accuracy</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Iris</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>6H.1M.2L</td>
</tr>
<tr>
<td>Palm Vein</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Human Retina</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>5H.1M.3L</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>7H.2M.0L</td>
</tr>
<tr>
<td>Ear</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>4H.5M.0L</td>
</tr>
<tr>
<td>Signature</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Gait Recognition</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>3H.5M.1L</td>
</tr>
<tr>
<td>Acoustic and Visual Features</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>4H.3M.1L</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>3H.6M.0L</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>3H.3M.3L</td>
</tr>
<tr>
<td>Teeth</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>2H.5M.2L</td>
</tr>
<tr>
<td>Skin Texture</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>3H.4M.2L</td>
</tr>
<tr>
<td>Footprint</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>2H.7m.0L</td>
</tr>
<tr>
<td>DNA Biometric</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>8H.1M.0L</td>
</tr>
<tr>
<td>Additional Biometrical Information</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>4H.4M.1L</td>
</tr>
</tbody>
</table>

**TABLE 18. COMPARISON OF OTHER BIOMETRIC TRAITS**

We can also measure the accuracy of access and identification of people through different algorithms and different biometric characteristics, by making a comparison between the research results and the references used, as in the

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Collectability</th>
<th>Circumvention</th>
<th>Ease Of Use</th>
<th>Accuracy</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Iris</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>6H.1M.2L</td>
</tr>
<tr>
<td>Palm Vein</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Human Retina</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>5H.1M.3L</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>7H.2M.0L</td>
</tr>
<tr>
<td>Ear</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>4H.5M.0L</td>
</tr>
<tr>
<td>Signature</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>7H.1M.1L</td>
</tr>
<tr>
<td>Gait Recognition</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>3H.5M.1L</td>
</tr>
<tr>
<td>Acoustic and Visual Features</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>4H.3M.1L</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>3H.6M.0L</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>3H.3M.3L</td>
</tr>
<tr>
<td>Teeth</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>2H.5M.2L</td>
</tr>
<tr>
<td>Skin Texture</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>3H.4M.2L</td>
</tr>
<tr>
<td>Footprint</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>2H.7m.0L</td>
</tr>
<tr>
<td>DNA Biometric</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>8H.1M.0L</td>
</tr>
<tr>
<td>Additional Biometrical Information</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>4H.4M.1L</td>
</tr>
</tbody>
</table>

**IV. RESULTS**

From the above tables it becomes widely clear to us that some of the biometric properties have been used, despite some defects in their use, such as the use of the face feature in facial recognition, as the available sources are many in this regard, which shows the extent of the method’s spread and ease of use and does not require special devices or contact with the person to be identified. But at the same time, we notice in this way some defects, for example, some external camouflage may affect the image of the face and the characteristics of the face may change, especially with the spread of plastic surgery and others. While we note other qualities with which sources have been scarce in dealing with artificial intelligence, such as the feature of DNA, which is one of the most important criminal characteristics in the event of biological effects of the intruder, and that this feature has been used for a long time in the detection and identification of criminals, and it does not require a lot of accurate devices For this, we note from the table below(table 4) that it is the most extensive, familiar and stable feature with the passage of time among all other biometric traits, as it showed the total degrees of positive traits for it 8H, but for ease of use trail the DNA will need some of precision devices for checking.

Also, through the obtained results, it is possible to isolate the biometric traits in which the level of their criteria is low despite the high rate of identification in them, such as (Teeth,
Footprint=2H). The reason for this is due to the difficulty of obtaining the person’s data or the loss of characteristics over time, such as the exposure of teeth to extractions, and the need for devices to take x-rays, and this is not available in places to be protected, but only for medical purposes. Also, the footprint is difficult to use if the intruder wears shoes.

Also for biometric traits that collect high points in recognition in addition to many high-score criteria such as (Human Iris, Palm Vein, Fingerprint, Signature=7H), (Human Retina=5H), They are reliable biometric traits and their results are never underestimated, because they are often fixed in humans and cannot be changed, imitated or manipulated easily, and they are familiar and recognized for a long time and recognized in many institutions that need high security with some failures sometimes or the need for smart devices and sometimes customized. As for the other biological traits, which are considered among the best and least widely used traits, they are (Ear, Acoustic and visual features, Additional biometrical information=4H), (Gait Recognition, Hand Geometry, Voice, Skin texture =3H), They are special characteristics that may need information taken closely by precise devices, or you need devices to take and obtain the intruder’s information, and collecting data in them is not easy, nor is it commonly used among people and may undergo rapid changes such as voice, hand, distortions and skin texture, so it cannot be relied on. These traits are generally used to identify intruders, although researchers have been able to reach high degrees of accuracy in discrimination. As for the algorithms used, most of what is used for the purposes of identifying people are neural network algorithms of various kinds, for several reasons, including:[57][60]:

1. The NN algorithm simulates the human neuron, which makes it more intelligent than the algorithms that simulate the intelligence of animals or insects. It is the part that affects the level of learning and recognition in it greatly.
2. When deep neural networks are used, they are widely expressive models.
3. From its tested results, neural networks are considered the most developed and successful in visual and audio recognition issues.
4. One of the most important successes of this algorithm is the ability to learn unexplainable solutions that may have unfamiliar or intuitive properties.
5. We also find that there is no distinction between single high-level units and linear random combinations of those units, the search space is considered to contain the semantic information and not the individual units in their upper layers of the neural network.
6. The deep neural network can learn the assignments of input and output in a large amount and in a short time. The best results, the best biometric properties, and the best algorithms used by researchers can be followed through tables (20,21).

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Highest degree</th>
<th>Highest accuracy</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Iris</td>
<td>7H</td>
<td>96%</td>
<td>NN</td>
</tr>
<tr>
<td>Face</td>
<td>6H</td>
<td>100%</td>
<td>NN</td>
</tr>
<tr>
<td>Palm Vein</td>
<td>7H</td>
<td>99%</td>
<td>Practical swarm intelligent</td>
</tr>
<tr>
<td>Human Retina</td>
<td>5H</td>
<td>99%</td>
<td>NN</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>7H</td>
<td>99%</td>
<td>Genetic</td>
</tr>
<tr>
<td>Ear</td>
<td>4H</td>
<td>98.8%</td>
<td>NN</td>
</tr>
<tr>
<td>Signature</td>
<td>7H</td>
<td>99.5%</td>
<td>NN</td>
</tr>
<tr>
<td>Gait Recognition</td>
<td>3H</td>
<td>96%</td>
<td>Practical swarm intelligent</td>
</tr>
<tr>
<td>Acoustic and visual features</td>
<td>4H</td>
<td>99%</td>
<td>Ant algorithm</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>3H</td>
<td>99.50%</td>
<td>ANN</td>
</tr>
<tr>
<td>Voice</td>
<td>3H</td>
<td>100%</td>
<td>ANN</td>
</tr>
<tr>
<td>Teeth</td>
<td>2H</td>
<td>98.8%</td>
<td>PSO</td>
</tr>
<tr>
<td>Skin texture</td>
<td>3H</td>
<td>90.10%</td>
<td>Neuro Fuzzy</td>
</tr>
<tr>
<td>Footprint</td>
<td>2H</td>
<td>96.25%</td>
<td>NN</td>
</tr>
<tr>
<td>DNA biometric</td>
<td>9H</td>
<td>99.60%</td>
<td>NN</td>
</tr>
<tr>
<td>Additional biometrical info</td>
<td>4H</td>
<td>100%</td>
<td>ANN</td>
</tr>
</tbody>
</table>

**Conclusion**

By following up on previous studies on the subject, we found several important points, First, we notice the frequent use of deep neural networks recently of all kinds, the most important of which are ANN and NN, as they involve processing huge data in a relatively short time, second not resort to algorithms that simulate animals a lot except for some research (like PSO, cuckoo search algorithm, etc.) for many reasons, the most important of which is that their steps are long and take a long time to implement, especially with large data often, and in the other hand, the ease of using neural networks, which are supported by most modern programming languages. also, most researchers resort to using biometric features whose data is easy to obtain for research and development especially data that can be taken by ordinary cameras. Which reduced the flow up and development of the use of other biometric properties, even if they have stronger specifications. In this paper, the most important biometric characteristics were discussed through several analogs. In the future we can compare the same biometrical features from other standers such that [35]: Property invariance, Measurability, Singularity, Reducibility, Tamper-resistance and reliability, Privacy, Comparable, Inimitable.
Acknowledgement

The authors would express they're thanks to college of Computer Sciences and Mathematics, University of Mosul to support this report.

References


[37] Benziane, Sarah Hachemi, and Abdelkader Benyettou. "Dorsal hand vein identification based on binary particle swarm


### TABLE 19. RESULTS OF FOR DIFFERENT ALGORITHMS

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Reference</th>
<th>Algorithm</th>
<th>Acceptance rate</th>
<th>Error rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Iris</td>
<td>[7]</td>
<td>feed forward ANN</td>
<td>93.33%</td>
<td>6.67%</td>
</tr>
<tr>
<td></td>
<td>[44]</td>
<td></td>
<td>96%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>[61]</td>
<td></td>
<td>74%</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>[62]</td>
<td></td>
<td>98.62%</td>
<td>1.48%</td>
</tr>
<tr>
<td></td>
<td>[73]</td>
<td>capsule network</td>
<td>99.37%</td>
<td>0.63%</td>
</tr>
<tr>
<td></td>
<td>[3, 65]</td>
<td>Deep learning algorithms</td>
<td>88.13%, 82%</td>
<td>11.87,12%</td>
</tr>
<tr>
<td></td>
<td>[8], [30]</td>
<td>Artificial neural networks</td>
<td>100%, 95.42%, 94.32%, 98.76%</td>
<td>0%, 4.58%, 5.68,1.24</td>
</tr>
<tr>
<td></td>
<td>[15]</td>
<td>Support vector machine</td>
<td>77%</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>[19]</td>
<td>CMNN</td>
<td>95%</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>[23]</td>
<td>AdaBoost, ANN</td>
<td>96.57%</td>
<td>3.43%</td>
</tr>
<tr>
<td></td>
<td>[32]</td>
<td>Feed-forward NN</td>
<td>95%</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>[51]</td>
<td>Cuckoo search algorithms</td>
<td>99.25%</td>
<td>0.75%</td>
</tr>
<tr>
<td></td>
<td>[63]</td>
<td>NN</td>
<td>98.88%</td>
<td>1.12%</td>
</tr>
<tr>
<td>Face</td>
<td>[1]</td>
<td>k-Nearest Neighbors</td>
<td>98%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>[6]</td>
<td></td>
<td>97.5%</td>
<td>2.5%</td>
</tr>
<tr>
<td></td>
<td>[37]</td>
<td>Practical swarm intelligent</td>
<td>99%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>[64]</td>
<td>CNN</td>
<td>99%</td>
<td>1%</td>
</tr>
<tr>
<td>Human Retina</td>
<td>[4]</td>
<td>Neural Network</td>
<td>99%</td>
<td>0.3% - 0.5%</td>
</tr>
<tr>
<td></td>
<td>[17]</td>
<td>fuzzy logic and NN</td>
<td>98.20%</td>
<td>1.74%</td>
</tr>
<tr>
<td></td>
<td>[59]</td>
<td>CNN</td>
<td>98.8%, 100%</td>
<td>1.2%, 0.0%</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>[5]</td>
<td>Genetic</td>
<td>99%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>[67]</td>
<td></td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>[74]</td>
<td>CNN</td>
<td>95.7%</td>
<td>4.3%</td>
</tr>
<tr>
<td>Ear</td>
<td>[2]</td>
<td>Nearest Neighbor</td>
<td>98.8%, 97.9%, 95%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>[46], [75], [76]</td>
<td>Convolutional NN</td>
<td>99%</td>
<td>1.2%, 2.1%, 5%</td>
</tr>
<tr>
<td>Signature</td>
<td>[9]</td>
<td>Feed Forward NN</td>
<td>99.5%</td>
<td>0.5%</td>
</tr>
<tr>
<td></td>
<td>[16], [29], [66]</td>
<td>Neural Networks</td>
<td>95.5%, 89.8%, 97.5%, 97.79%, 82.5%, .75%, 75%</td>
<td>5%, 10.2%, 2.5%, 2.21%, 17.5%, 1.5%, 15%</td>
</tr>
<tr>
<td></td>
<td>[20], [45]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[22]</td>
<td>particle swarm and NN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[24]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gait Recognition</td>
<td>[10]</td>
<td>ANN</td>
<td>96%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>[14], [26]</td>
<td>Particle swarm optimization</td>
<td>94.37%</td>
<td>5.63%</td>
</tr>
<tr>
<td></td>
<td>[31]</td>
<td>Pairing NN</td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td>[72]</td>
<td>ENN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acoustic and Visual Features</td>
<td>[11]</td>
<td>HyperBF networks</td>
<td>91.9%, 98%</td>
<td>9%, 2%</td>
</tr>
<tr>
<td></td>
<td>[36]</td>
<td>Neural network</td>
<td>93.5%</td>
<td>6.5%</td>
</tr>
<tr>
<td></td>
<td>[48]</td>
<td>Ant lion algorithm</td>
<td>99%</td>
<td>1%</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>[12], [42]</td>
<td>back propagation NN</td>
<td>87.237%, 95%</td>
<td>14.780%, 5%</td>
</tr>
<tr>
<td></td>
<td>[39], [41]</td>
<td></td>
<td>99.11%, 99.50%</td>
<td>0.89%, 0.5%</td>
</tr>
<tr>
<td></td>
<td>[68]</td>
<td>BPNN</td>
<td>93%</td>
<td>7%</td>
</tr>
<tr>
<td>Voice</td>
<td>[18], [28]</td>
<td>Convolutional NN</td>
<td>92.1%, 100%</td>
<td>7.9%, 0%</td>
</tr>
<tr>
<td></td>
<td>[69]</td>
<td>Fuzzy and NN</td>
<td>94%</td>
<td>6%</td>
</tr>
<tr>
<td>Teeth</td>
<td>[21]</td>
<td>ANN</td>
<td>81.69%</td>
<td>18.31%</td>
</tr>
<tr>
<td></td>
<td>[43]</td>
<td>Multiple intelligent algorithms</td>
<td>83.5%</td>
<td>16.5%</td>
</tr>
<tr>
<td></td>
<td>[47], [49]</td>
<td>PSO, contourlet particle swarm optimization</td>
<td>98%, 98%</td>
<td>2%, 2%</td>
</tr>
<tr>
<td>Skin Texture</td>
<td>[13]</td>
<td>Neuro Fuzzy Inference</td>
<td>90.10%</td>
<td>9.9%</td>
</tr>
<tr>
<td></td>
<td>[27]</td>
<td>particle swarm algorithm</td>
<td>90%</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>[70]</td>
<td>NN</td>
<td>96%</td>
<td>4%</td>
</tr>
<tr>
<td>Footprint</td>
<td>[53], [54]</td>
<td>NN</td>
<td>96.25%, 78%</td>
<td>4.75%, 22%</td>
</tr>
<tr>
<td></td>
<td>[71]</td>
<td>KNN</td>
<td>99.30%</td>
<td>0.7%</td>
</tr>
<tr>
<td>DNA</td>
<td>[34]</td>
<td>particle swarm algorithm</td>
<td>93%</td>
<td>7%</td>
</tr>
<tr>
<td></td>
<td>[56]</td>
<td>NN</td>
<td>99.60%</td>
<td>0.40%</td>
</tr>
<tr>
<td></td>
<td>[77]</td>
<td>CNN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Biometrical</td>
<td>[33]</td>
<td>intelligent neural network</td>
<td>96.6%</td>
<td>3.4%</td>
</tr>
<tr>
<td></td>
<td>[40]</td>
<td>SVM and MLP</td>
<td>94.1%</td>
<td>5.9%</td>
</tr>
<tr>
<td></td>
<td>[50]</td>
<td>smart techniques</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>[52]</td>
<td>Fuzzy system</td>
<td>95.7%</td>
<td>4.3%</td>
</tr>
<tr>
<td></td>
<td>[55]</td>
<td>ANN</td>
<td>100%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
الملخص

تحدث العديد من حالات السرقة والتهدي على الممتلكات بالإضافة إلى الجرائم في العالم بعد اقتحام الأشخاص لممتلكات الناس ومتاجتهم بشكل غير قانوني، لذلك يهدف هذا البحث إلى إلغاء ضوء على معظم الأساليب الذكية وتكنولوجيا الكمبيوتر المستخدمة في التعرف على الأشخاص التي تساعد على التقليل من هذه الجرائم. حيث تم الاعتماد على نموذج التعرف البصري، مثل بصمة الأصابع، بصمة اليد، والأذن، والوجه، والملمس، وبعض التشوهات المميزة للأشخاص، والعين، وآثار الأقدام، وتحليل الجروح الفطرية من الأشخاص، وغيرها من النماذج الحيوية المهمة. أيضًا، تم استخدام العديد من الخوارزميات الذكية لتحديد هذه السمات.

الكلمات المفتاحية: الخصائص البصريه، ذكاء سرب الجسيمات، الشبكات العصبية.