H2020 – BES – 5 – 2015

Research Innovation Action

Intelligent Portable ContROl SyStem

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626

D3.1 Data Collection Devices - specifications

Report Identifier:	D3.1		
Work-package, Task:	WP3, T3.1	**Status – Version:**	1.00
Distribution Security:	PU	**Deliverable Type:**	R
Editor:	ITTI		
Contributors:	EVR, ED, ICCS, BIOSEC		
Reviewers:	ED, ICCS		
Quality Reviewer:	ED		
Keywords:	Data collection devices, sensors, DAAT, ADDS, FMT, human and vehicle detection, surveillance		
Project website: www.iborderctrl.eu			

Table of Contents

Abbreviations

ADDS	Automatic Deception Detection System
AWB	Automatic White Balance
BCAT	Integrated Border Control Analytics Tool
BCT	Biometric Capture Template
BET	Biometric Enrol Template
BSIF	Binarized Statistical Image Features
CCD	Charge Coupled Device
CST	Counter Spoofing Techniques
CT	Computed Tomography
DAAT	Document Authenticity Analysis Tool
DCT	Discrete Cosine Transform
DWT	Dicrete Wavelet Transform
EER	Equal Error Rate
EMC	ElectroMagnetic Compatibility
FAR	False Acceptance Rate
FMR	False Match Rate
FMT	Face Matching Tool
FNMR	False Non Match Rate
FRR	False Rejection Rate
HHD	Hidden Human Detection
HOG	Histogram of Gradient
iBorderCtrl	Intelligent Portable Control System
LBP	Local Binary Pattern
LBP	Local Binary Pattern

LPQA	The Local Phase Quantization Analysis
LRFA	Local-Ridge Frequency Analysis
MRZ	Machine Readable Zone
OCR	Optical Character Reading
PU	Portable Unit
RBAT	Risk Based Assessment Tool
SISII	Schengen Information System
VIS	Visa Information System
WDR	Wide Dynamic Range
WLD	Weber Local Descriptor

Executive Summary

The success of a biometric or scanning system, related to control procedures, often depends on choosing the right modality each task, but seems to be a rather complicated task. Careful research that includes rigorous comparisons of modality strengths and weaknesses is an important element to help select the right hardware. More specifically there are some important factors which should be considered before choosing a sensor or device. These include: accuracy (based on several criteria including error rate, FAR, FRR, identification rate etc.), anti-spoofing capabilities (anti-spoofing protection is a must have capability for the right biometric modality), user acceptability (understanding which modalities are acceptable versus those that may cause user acceptance issues is important), cost effectiveness (depending on the underlying technology and hardware characteristics, certain modalities may be more cost effective than others), international standard and certification (there are international standards often required for large scale identification projects), compatibility (it is important that the devices are supported and compatible between the system's operating system and the deployed biometric software) and last but not least the exact device specifications[1].

It's important to realize that there is not one device/sensor which is best for all conditions and implementations. Many factors must be taken into account including location of operation, security, acceptability, deployment requirements, ease of use, accessibility taking also into consideration the working conditions of the people who will use the system on a daily basis and how they will use it. Hence, performance and cost may vary when taking into consideration the abovementioned factors. As an example, different industries need different types of biometric modalities based on different scenarios depending on the application context in which a biometric system is designed. Hence, choosing the right device/sensor is important to maximize the full benefits of a system as not all available hardware in the market has the ability to meet the requirements of the project[2].

The purpose of this deliverable is to identify the necessary hardware sensors – cameras, scanners and other sensors, which will be the staple of iBorderCtrl system. The carried-out review and device selection sections within this document provide valuable recommendations with regard to the hardware components that might be applied in the project. The selected devices will be considered during design and development phase of such modules as BIO, DAAT, ADDS, FMT, as well as HHD.

The hereby deliverable is, to a large extent, based on the previous work done within WP2 concluded with D2.1 and D2.2. This document provides content which is corresponding and compliant with the iBorderCtrl user requirements, technical requirements as well as system architecture. The deliverable further extends the border control related issues reported within D2.1 with an overview of spoofing techniques used by travellers. Furthermore, the report provides an in-depth review of biometric, hidden people detection and document readers' technologies. The technology description sections are concluded with a device recommendation for each iBorderCtrl component.

The hereby document, therefore, complements D2.1 and D2.2. Altogether, the three deliverables constitute a solid base for the development of iBorderCtrl components.

[1] http://www.m2sys.com/blog/biometric-hardware/5-factors-consider-choosing-best-biometric-modality/
[2] http://www.m2sys.com/blog/biometric-hardware/secret-behind-choosing-the-best-biometric-scanner/

1 Introduction

1.1 Purpose of this Document

This report describes works carried out within Task 3.1, which is devoted to identification of necessary hardware sensors to be exploited in iBorderCtrl tools.

The overall objectives of WP3 are to:

- adapt the physical sensors and hardware to be used for data collection,
- develop the automated real-time deception detection system (ADDS), the travel document authenticity analytics tool (DAAT), the face matching tool (FMT), the automated border control avatars,
- provide hidden human detection in vehicles as alert tool,
- design and implement the radio network to guarantee wireless connectivity and QoS.

The report D3.1 Data Collection Devices – specifications aims to deliver an in-depth review of available technologies that could be relevant for the iBorderCtrl system components. Providing a broad-spectrum analysis of state-of-the-art sensor technologies is essential when considering such a complex system as iBorderCtrl. Moreover, the indication of existing technologies is believed to help in identification of strengths and weaknesses of relevant technologies. The report further defines particular sensors, which should be considered as a basis for system components development. The ultimate choice with regard to the technology selection is made by each component development leader.

The work carried out within T3.1 is inherently connected to the previous work done as a part of WP2 tasks such as T2.1 and T2.2, which dealt with the analysis of user requirements and definition of use case scenarios as well as development of reference architecture. The hereby deliverable is built on the knowledge reported in D2.1, in particular the section on current state-of-the-art technologies and systems used by border guards. However, D3.1 goes largely beyond the description level included in D2.1 and provides valuable information related to the usefulness of researched technologies and their technical specification. What is more, D3.1 covers the aspect of spoofing possibilities and describes a real life scenarios, to give insight into the potential obstacles that iBorderCtrl system might face in operational conditions.

Furthermore, D3.1 is closely linked with D2.2 as well. D2.2 constitutes a significant input to the hereby report with regard to the system architecture and technical requirements. D3.1 presents each component description with a set of corresponding functional requirements. In general, D3.1 combined with previous reports mentioned in the text above gives a holistic view upon border control related issues, expectations from the new system, as well as iBorderCtrl solution.

Therefore, it is believed that D3.1 will remain a solid base for other tasks within WP3 that are related to the development of system components including ADDS, DAAT, BIO, FMT, and HHD.

1.2 Structure of the Document

The structure of this document is as follows:

- **Section 2** provides practical insight into spoofing techniques that are used by people illegally trying to cross borders. Examples are based on real-life situations. As a complementary part of the section, the comprehensive analysis of counter-spoofing methods has been provided, focusing on both hardware and software techniques.

- **Section 3** comprises a complete description and analysis of all biometric scanners, which include fingerprint, face and vein sensors. The descriptions begin with background information on their functioning and present reference to the iBorderCtrl system architecture. Then, several sensors and devices for extracting particular biometric feature have been listed and their SWOT analyses presented. On that basis, the final selection of desired biometric scanner is made.
- **Section 4** focuses on document authentication instruments. Main tools of interest include RFID chip readers, QR code scanners and document scanners. The output of this analysis will be used to select the best set of devices for DAAT.
- **Section 5** gives an overview on tablet devices that might be used by border guards during the collection of biometric data and for checking all required documents. This section is structured in the similar way as biometric devices, presenting reference to requirements and giving the overview and final selection of the device to be used as a central module in the Portable Unit.
- **Section 6** provides the description of surveillance instruments for iBorderCtrl solution. Several technologies for detecting hidden people are discussed and recommendations are provided.
- **Section 7** provides conclusions stemming from the document.

2 Spoofing and counter spoofing techniques in biometrics

2.1 Introduction – Overview

Before presenting the selection of all data collection devices (scanners, sensors, readers) in the following Chapters, for the various modules that consist the iBorderCtrl system, it is considered wise and useful to tackle the various aspects referring to the possible techniques used for deceiving the control devices especially in Biometrics. To this respect, the subject of the present Chapter 2 is to provide a brief but essential overview of the spoofing and respectively of the counter-spoofing techniques particularly in the fingerprints, palm vein and face recognition control systems that can be used in the framework of BCP control checks.

The reason for that is, that the selection of especially the biometrics devices (fingerprints, palm vein and face recognition scanners) greatly depends on the ability of the relevant systems (taking into account both hardware and software) to withstand and in certain cases to detect possible attempts of deception. Since a large variety of corresponding sensors is available commercially, as it will be seen in the Chapters to follow, addressing various technologies, it is of great importance that the selection of the specific devices within the iBorderCtrl complies with the prerequisites for anti-spoofing.

Especially, the selection of the fingerprints scanners, apart from the rest of the performance criteria involved, needs to be also determined by their ability to encounter anti-spoofing functionalities; and this is important since, as also dealt in D2.2, the fingerprints checks are currently the only mandatory biometric check at the BCPs, especially for the TCNs, while palm vein and face recognition checks are the most promising candidates for relevant implementation in the near future.

However, it is not the intention of this Chapter to provide a thorough insight of the best possible spoofing and especially counter-spoofing techniques available worldwide, neither to suggest the development of the optimal relevant solution. After all, it is more than clear that the iBorderCtrl project does not involve the development of advanced biometrics scanners; this kind of developments are outside the IBorderCtrl's scope. The ambition of the project is not to result in enhanced biometrics scanners with innovative anti-spoofing solutions but to effectively integrate those currently available to a holistic platform incorporating various Border Control systems and solutions.

After all, counter-spoofing techniques are already embedded in the currently available commercial fingerprints, palm vein and face recognition systems, either in the respective hardware or software in terms of marching algorithms. Thus, the main focus of the project is to include those most promising of the available mainstream pool of sensors incorporating counter-spoofing techniques as an additional important specification specifically for implementation at the BCPs control checks.

Based on the above, Chapter 2 provides a brief but comprehensive overview of the relevant available techniques based on the related academic and commercial literature and the partners experience. Two are the main reasons for including this approach within this Deliverable: firstly, to facilitate the reader for better understanding both the operation of each of the biometric sensors and their technological principles but also the rationale behind incorporating anti-spoofing. And secondly, to guide the selection process of the subsequent Chapters and to define the main prerequisites in terms of tackling deception that should be investigated among the commercial systems.

It should be noted, the present Deliverable D3.1 deals mostly with the selection of the hardware biometrics devices while the overall modules including the matching algorithms and software techniques will be dealt in the following Deliverable D3.2. To this respect, the present Chapter acts as an appropriate introduction to all the relevant aspects tackled in both these Deliverables.

2.1.1 Spoofing phenomena at the BCPs – rationale

Prior to the development and implementation of large scale systems based on biometric verification, it is essential to consider the aspect of spoofing. Spoofing, which is an intentional act of deceiving the system has been a major concern of industry representatives, legislative bodies as well as regular security/border officers. Regular attempts to spoof biometric verification systems at EU/Schengen borders have ignited initiatives and research on counter-spoofing techniques. The present chapter, therefore, presents spoofing techniques, especially those related to fingerprint, vein and face recognition. To give it more credibility, the text reflects real life spoofing scenarios, which have been registered at Hungarian border crossing points along with the description of the relevant counter spoofing methods to indicate the severity of the problem.

Currently, the most trending way of illegal border crossing is to cross the "green border"[3] which requires advanced surveillance tools and methods in an extended borderline. The second most relevant modus operandi is hiding in vehicles, especially nowadays with the dramatic increase in illegal migration, while the third most significant trend of illegal border crossing is impersonation. However, it should be noted that the first two trends are mostly affected by the external political situations, presenting periods where these phenomena may show dramatic upsurge (in case of civil wars as recently drawn by the war in Syria) or remarkable diminution i.e. in post conflicts situations.

Impersonation on the other hand, presents a continuously used illegal way over the years and may result in advanced and sophisticated spoofing methods especially when terrorism is involved; in this sense its inherently personal manner affects a large variety of checking and control methods, which may result in a wider uptake when considering terrorist threats over the years and the increased need for counter spoofing techniques respectively. **To this respect, the impersonation trend presents greater significance and thus, from the viewpoint of iBorderCtrl, impersonation and connected spoofing is an important aspect to be dealt with.**

Suspects take passports and/or other documents of someone else looking alike and try to get past the border check. As evidence of the continuous efforts held at the BCPs, up to the current date any kind of attempts related to impersonation by spoofing the RFID chip in the biometric passport are hardly detected; however, with the technology advancements, this may just be another barrier that will be soon overcome. Among the other biometric identifiers, fingerprints are the only ones used nowadays regularly at the borders; therefore, a small number of people still try to "get rid" of their fingerprints using different methods. Fake fingerprints have not been detected yet, although in general there are several known methods to spoof fingerprints on sensors in possession of the attacker. Based on the above, it can be stated that, currently, face recognition is the most relevant element of the system, however, new biometrics, especially vein pattern can create a non-erasable and almost impossible to spoof solution for identification of persons.

Considering the above trends and practices, it seems useful to provide an insight into available spoofing methods and, subsequently, have them in mind when selecting the appropriate biometric scanning devices.

---

[3] Green border is the external land borders outside BCP areas. Blue border is any external water border (maritime, river, or lake), as appears in "BETTER MANAGEMENT OF EU BORDERS THROUGH COOPERATION - Study to identify best practices on the Cooperation between Border Guards and Customs Administrations working at the external Borders of the EU", 2011, Center for the Study of Democracy, Bulgaria, ISBN: 978-954-477-169-0, following the "European Commission Communication of 7 May 2002 on integrated border management" and the "Feasibility study of 30 May 2002 on a European Border Police" relevant documents.

2.2 Spoofing Techniques Analysis

Biometric recognition refers to identifying or verifying the identity of a person based on physical or behavioural characteristics such as fingerprints, face. Given the current classification, eight possible methods of attack on biometric sensor systems are identified[4].

1. Presenting a fake biometric to the sensor (spoofing);
2. Resubmitting previously intercepted biometric signals, bypassing the sensor;
3. Overriding the feature extraction process (using a Trojan horse, the feature extraction module produces feature sets selected by the attacker);
4. Replacing the features extracted from the input signal with a different feature set;
5. Corrupting the matcher (to output preselected matching scores);
6. Tampering with the template database (injection of a new template, overwrite or remove an existing template);
7. Modifying the templates transmitted through the channel between the template database and the matcher;
8. Altering the final decision (the matcher result is overridden by the attacker).

Taking the biometric trait attributes into consideration, the attacks at the biometric sensor level can be classified as summarized in the following table.

Table 1 Attacks at the biometric sensor level

Type of attack	Type of biometric trait	Owner of the trait	Modification of the trait
Spoofing	Fake sample	-	-
Dismembered body parts	Real sample	Legitimate user	Unmodified
Coercion	Real sample	Legitimate user	Unmodified
Obfuscation	Real sample	Attacker	Modified
Mimicry	Real sample	Attacker	Modified
Targeted impersonation	Real sample	Attacker	Unmodified
Casual impersonation	Real sample	Attacker	Unmodified

2.2.1 Fingerprint recognition

2.2.1.1 Basis information for fingerprint authentication

To understand how fingerprint readers and algorithms operate, some basic knowledge on dactyloscopy is needed, presented in the following:

Basic patterns: The fingerprints are the impression of the friction ridges and furrows which appear in the pads of the fingers and thumbs. These friction ridge patterns are grouped into three distinct types—loops, whorls, and arches—each with unique variations, depending on the shape and

[4] N. K Ratha, J. H. Connell, R. M. Bolle. 1999. *A Biometrics-Based Secure Authentication System*, pp. 70-73.

relationship of the ridges. The loops are the prints that recurve back on themselves to form a loop shape. The loops account for approximately 60% of the pattern types. The whorls form circular or spiral patterns and it can be divided in four different subtypes. They refer to about 35% of patterns types. The arches create a wave-like pattern and include plain arches and tented arches, representing about 5% of all pattern types.

Minutiae features: The specific points of a fingerprint are called minutiae. Since these are the reference points for fingerprint recognition, they are the most important for the result and security score of the authentication. The minutiae features can be divided into three main categories: the bifurcation, ridge ending and the dot[5].

Figure 1 Typical fingerprint patterns

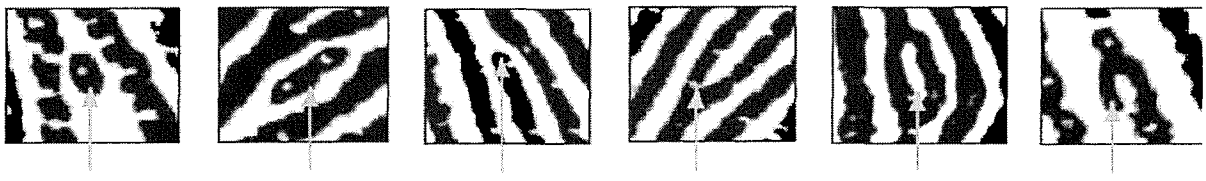


Figure 2 Typical ridge patterns

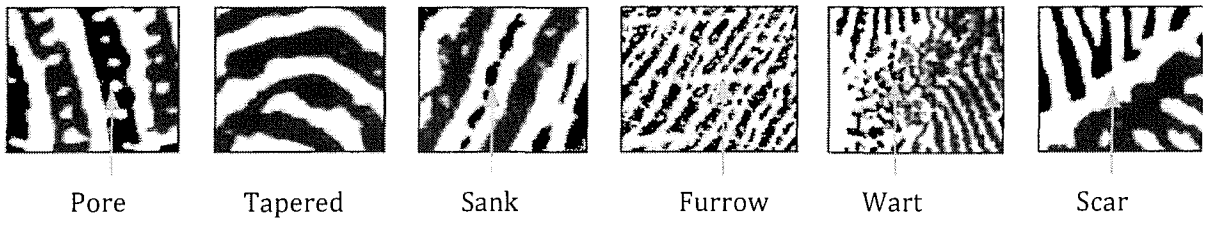


Figure 3 Typical ridge patterns (contd.)

How fingerprints are compared: The analyst first uses the general pattern type (loop, whorl or arch) to make initial comparisons and include or exclude a known fingerprint from further analysis. To match a print, the minutiae is used to identify specific points on a fingerprint comparing them with the template. Then specific matched information within the minutiae is identified and if enough details correlate, it is determined that the fingerprints belong to the same person. All the best available fingerprint matching algorithms obtain and compare the different minutia points from each fingerprint template resulting to a matching score. If this score is above a defined threshold then the

[5] D. Maltoni, D. Maio, A. Jain, S. Prabhakar. 2009. *Handbook of Fingerprint Recognition.* Springer.

match is positive. In order to increase the level of accuracy all ten (10) fingerprints from all fingers can be used; thus providing a lower FAR (False Acceptance Ratio) by increasing the total number of minutiae compared.

Fingerprint Spoofing: The applications of fingerprint-based systems and devices has largely proliferated in recent years. Fingerprints are the key feature for passenger authentication at border crossing points, criminal investigations, access control systems, banking systems, and numerous other areas. Moreover, the technological achievements in sensor miniaturization enables the incorporation of fingerprint-based modules in such devices as laptops and mobile devices. Though the fingerprint itself is a highly unique and reliable feature, it should be noted that numerous techniques emerged enabling spoofing of the fingerprint-based biometric systems. Fingerprint spoofing methods present a large variety since people are trying to evade the fingerprint identification process' by temporarily (or permanently) "removing" their fingerprints by burning them with fire, acid or scratching them using sandpaper so that to avoid recordability.

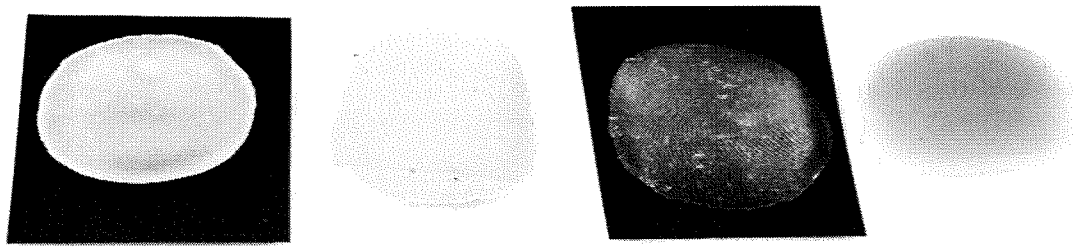


Figure 4 Samples of reproduced fingerprints[6]

Spoofing methods can be divided into co-operative and non-co-operative ones. The first relies on a direct attempt to deceive the system with a fingerprint sample made out of plastic, gelatine or clay. These materials are used to reproduce a person's fingerprint as a live finger mould (as in Figure 5) when interacting with the system. Non-cooperative spoofing on the other hand, includes several types such as latent fingerprint and fingerprint reactivation. Latent fingerprints are the marks left by a person on a certain object, which might not be visible at first. To fully recover a latent fingerprint, the mark is covered with powder and the excess is swept with a brush. Projecting UV light on the fingerprint reveals the details of the mark and thus, the latent fingerprint can be collected and digitized. Fingerprint reactivation is the application of the latent fingerprints deposited on the sensor[7].

2.2.2 Face recognition

There is a number of technologies for face recognition on the market such as 2D, 3D, NIR and thermal vision cameras. Existing solutions offer satisfactory results in terms of performance and accuracy. However, similarly to fingerprint verification, face recognition systems has also drawn the attention of attackers. There have been several spoofing methods that are proven to cause difficulties for face recognition systems. First of all, printed face photographs of a different person have been successfully used to deceive the system, which theoretically is the most simplistic method of varication. Over time, the applied methods have become more sophisticated. Attempts to spoof the face recognition systems are made with digital photographs displayed on a device, video samples, and even 3D masks. Apart

[6] http://www.touchngoid.com

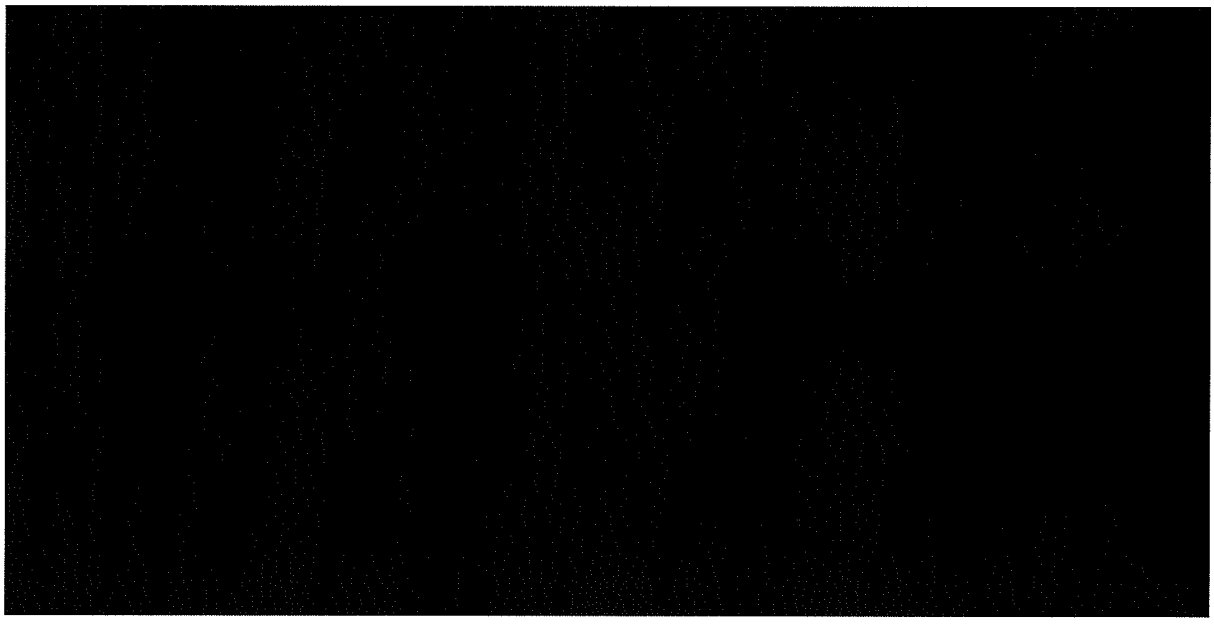
[7] S. Samruddhi, H. Y. Patil. *Survey on Fingerprint Spoofing, Detection Techniques and Databases,* International Journal of Computer Application (0975-8887).

from the above, impersonation attempts take also place with false or stolen documents, where photographs could resemble the attacker. Such cases are frequently detected on border crossing points; several of them are presented below[8].

Case studies about forgery of official documents – *spoofing identity: impersonation cases*

Case 1: the person (picture) in the passport delivered to the border guard is different from the person owning the document; The border guard found a significant difference between the person delivering the passport and the photo (portrait) in the travel document (as in the "fake" pictures below) resulting in more thorough inspection. The tools used during the thorough checking were signature pattern matching and making comparative photos.

Case 2: An ID card and a driving licence delivered by a woman are checked and the documents are different from their owner. The delivered ID card was original in all of its components but a significant difference was found between the ID card photo and the face of the woman delivering it. For a secondary checking other document (driving licence) was inspected resulting in the same conclusion. For checking, *UVEC PASS/D* device, digital microscope, camera, hand glass were used (mock-up examples are given below).

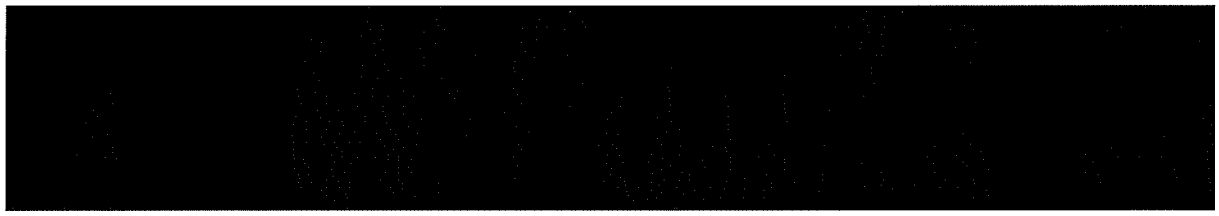


Case 3: This case is about a person was exiting from Hungarian BCP as a traveller of another EU country's vehicle. For checking he delivered his private passport made by TCN authorities as well as residence permit and driving licence made by the other EU country's authorities. During the checking, the birth date and birth place in the passport was not the same as in the other documents. Moreover, the person being checked gave wrong answers to the questions related to personal data as well as his signature was not the same with the signature in the documents. The difference between the photo and the face of the person delivering the passport was still noticeable. For checking, *UVEC PASS/D* device, digital microscope, camera, hand glass were used (as in the examples below)

[8] T. Bourlai. 2016. *Face Recognition Across the Imaging Spectrum.* Springer, pp. 165-168.

Case 4.: The example pictures below show an impersonation case with an EU biometric passport. A significant difference is found between the person delivering the passport and the photo (portrait) in the biometric travel document. Tools used for checking were 'HORUS 1019' and VSC 40/H devices.

Case 5.: The pictures below show another case about forgery of official documents – specialisation of mistaken identity cases. The border guards identified that the biometric private passport delivered was under alert as stolen in the Schengen Information System. Of course, also in this case a significant difference between the person delivering the passport and the photo (portrait) in the biometric travel document was evident.



2.2.3 Veins recognition

In case of palm vein scanners, spoofing attacks can be described as the-so called direct attacks; the sensor is attacked using synthetic biometric samples without requiring prior specific knowledge about the system. One of the most common spoofing technologies is using printed papers. In this case the main motivation is based on the fact that it is simple and easy to do, and it is already proved to be efficient in the context of other biometric modalities.

The process of the spoofing can be implemented with different tricks e.g. printing: all real images; two real palm vein images; just real palm vein image, etc. This is achieved by printing with a normal and commercial printer machine the real palm vein images without any kind of pre-processing on a regular paper and presented to the palm vein sensor; cases were reported in the past (as in the figure below) where the intruder was granted access to the system with a probability of spoofing false accept rate as high as 65%.

It is important to notice that nowadays, with the technology advancements, palm vein technology is among the safest ones, and deception of the relevant systems is not quite simple. Among all biometric technologies, human palm vein recognition has emerged as a reliable technology to provide greater level of security to personal authentication system. In various surveys, palm print verification experiments demonstrated the superiority of multispectral fusion to each single spectrum, resulting in both higher accuracy and anti-spoofing capability.

[redacted]

2.3 Counter-spoofing techniques analysis

Counter-spoofing techniques - CST (or, equivalently, anti-spoofing techniques, feature level techniques) can be divided into two versatile branches: hardware-based and software-based.

The software-based technology operates by assessing characteristics of the sample pattern. The most common anti-spoofing technique is based on the software image analysis. The main advantage of the software counter-spoofing techniques is that they do not require extra hardware devices and are easier to be implemented and updated (by the modification of the code). Also, novel approaches, such as machine learning may be easily employed.

Hardware-based technology of CST detects liveness of the analysed person by using characteristics of his/her vitality such as scent, pulse oximetry, blood pressure, temperature, conductivity and electrical resistance of the skin. Generally, hardware-based technology covers four approaches:

- Intrinsic properties of a living body (including physical properties – density, elasticity; electrical properties – capacitance, resistance; spectral properties – reflectance, absorbance at specific wavelengths).
- Involuntary signals of living body which make use of human nervous system – detection of the pulse, blood pressure, perspiration, pupillary unrest and electric heart signals.
- Challenge response methods, that include anti-spoofing with the user cooperation. They detect voluntary and involuntary reactions to an external signal.
- Multimodality, multibiometric CST use a combination of different techniques, such as finger vein along with fingerprint authentication.

The disadvantage of hardware-based anti-spoofing technologies is that they require additional hardware to detect particular properties of a living trait. Furthermore, added hardware results in an increased price of the device.

[redacted]

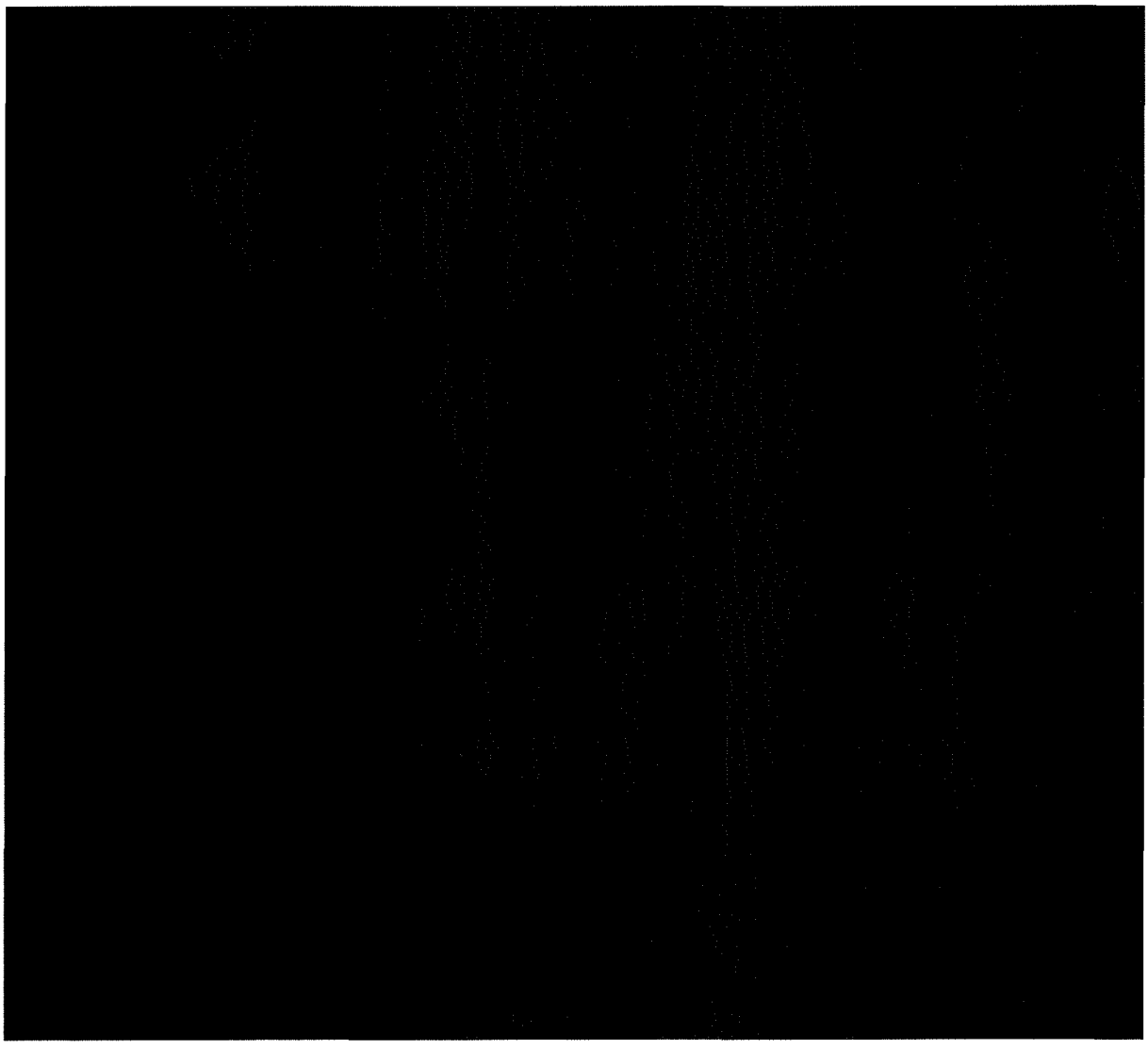
2.3.1 Fingerprint counter-spoofing

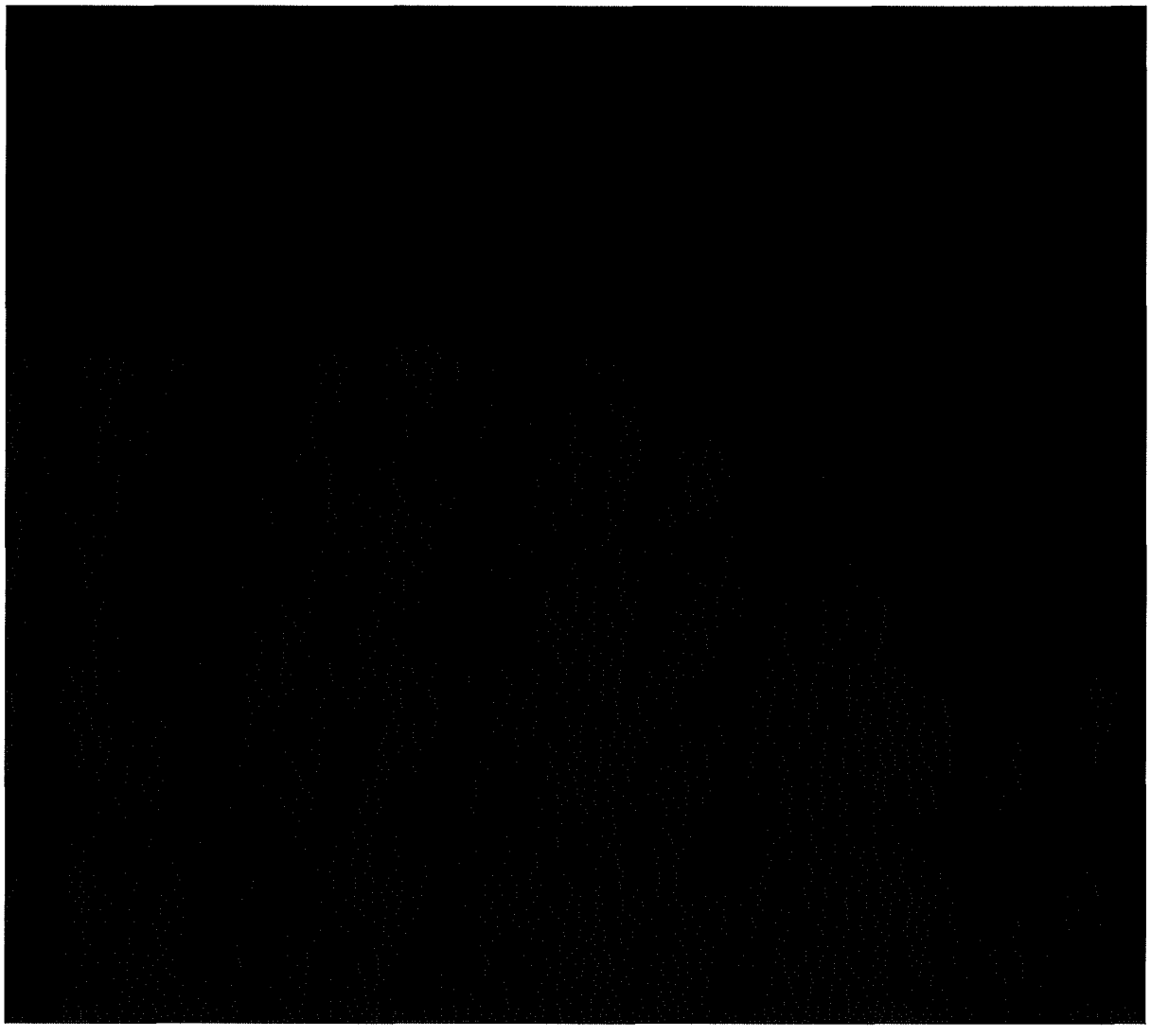
2.3.1.1 Hardware-based approach

Hardware-based techniques detect the vitality signs from the available biometric at the acquisition stage. They usually incorporate extra hardware to acquire life signs from the presented biometric sample. Integration of the new hardware devices increases the cost of the biometric system, moreover it is usually more invasive to users than other methods.

2.3.1.2 Software-based approach

Two types of the software-based technologies for counter-spoofing are present: **dynamic and static**. The first one makes use of dynamic behaviour of live fingertips such as ridge distortion or perspiration. On the other hand, static methods analyse texture or presence of pore and perspiration. Static methods are preferable than dynamic as they usually require less cooperation with the user, which makes them faster and less intrusive.

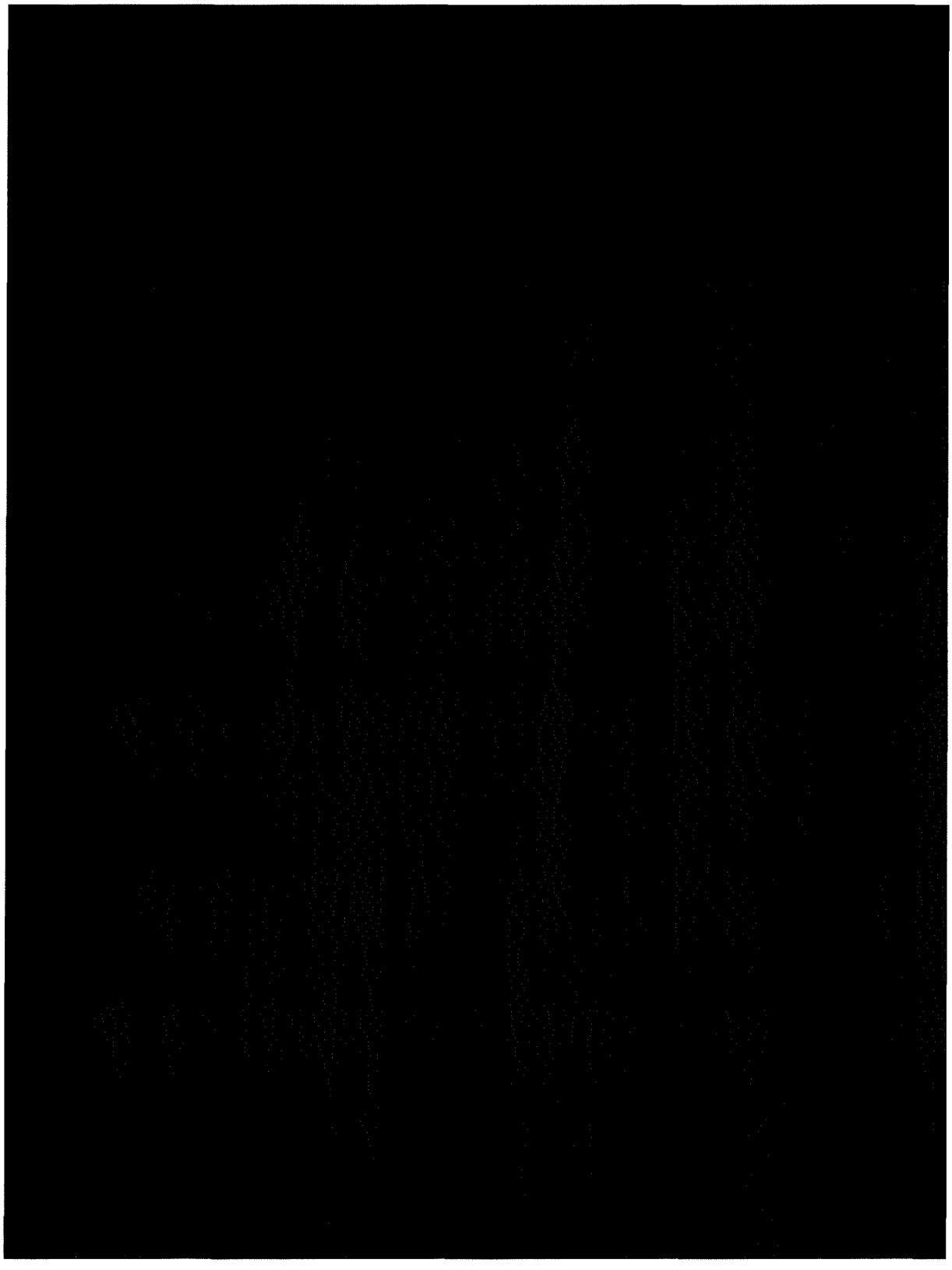


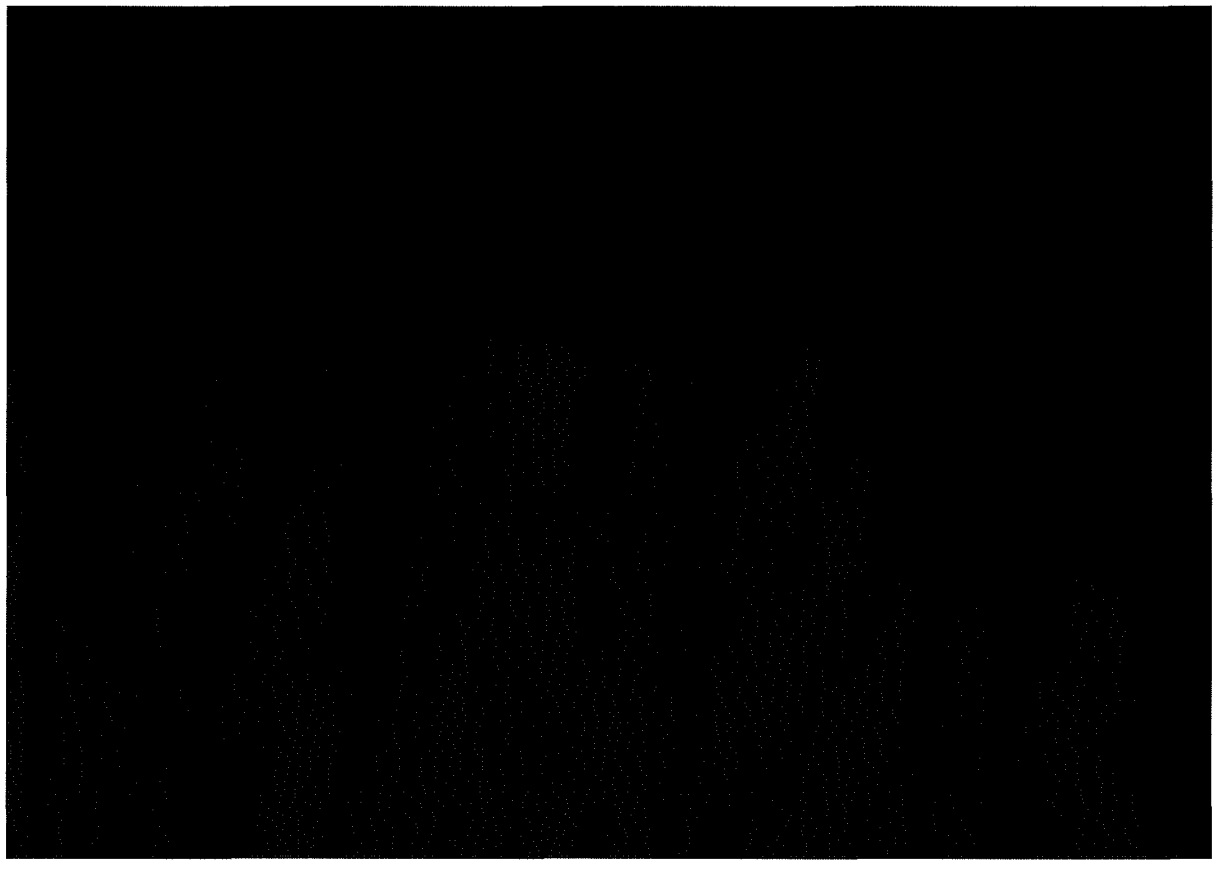


2.3.2 Face counter-spoofing

Descripted case studies about forgery of official identification document clearly indicate that the CST workflow must comprise the document scanning (document scanner device VIS) procedure and face capture (digital camera device) procedure. The process of the border checking consists of comparing two images, scanned portrait from the traveller id and captured face image during border checking procedure.

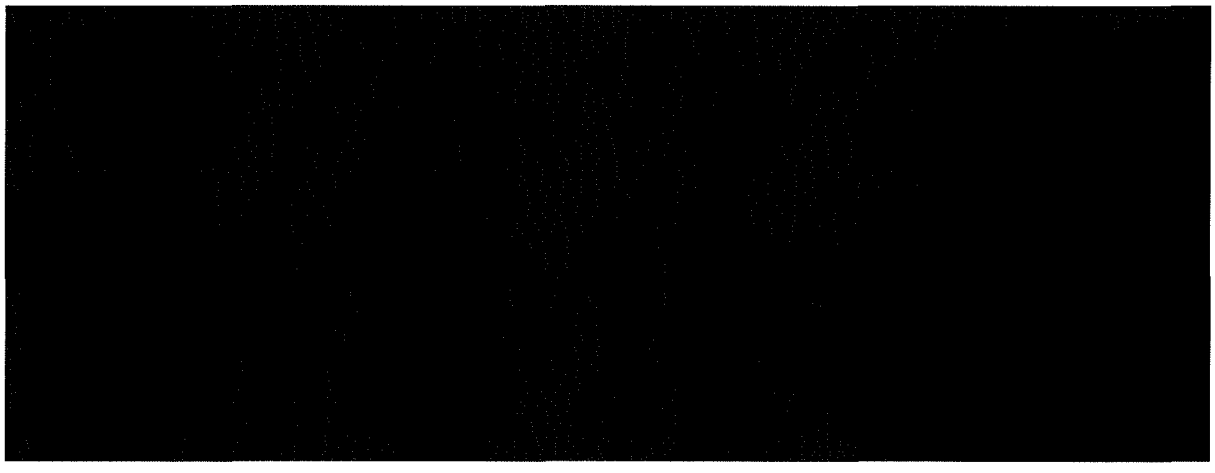
From definition, face counter-spoofing techniques detects liveness of the analysed user portrait, during the border crossing procedure to detect spoof through photograph or video. Therefore, methods described below focus mainly on the face recognition through the scanned document portrait of the traveller. In fact, the likelihood of the face mask detection by border guards is still high, although the CST that focus on live detection are described as well.

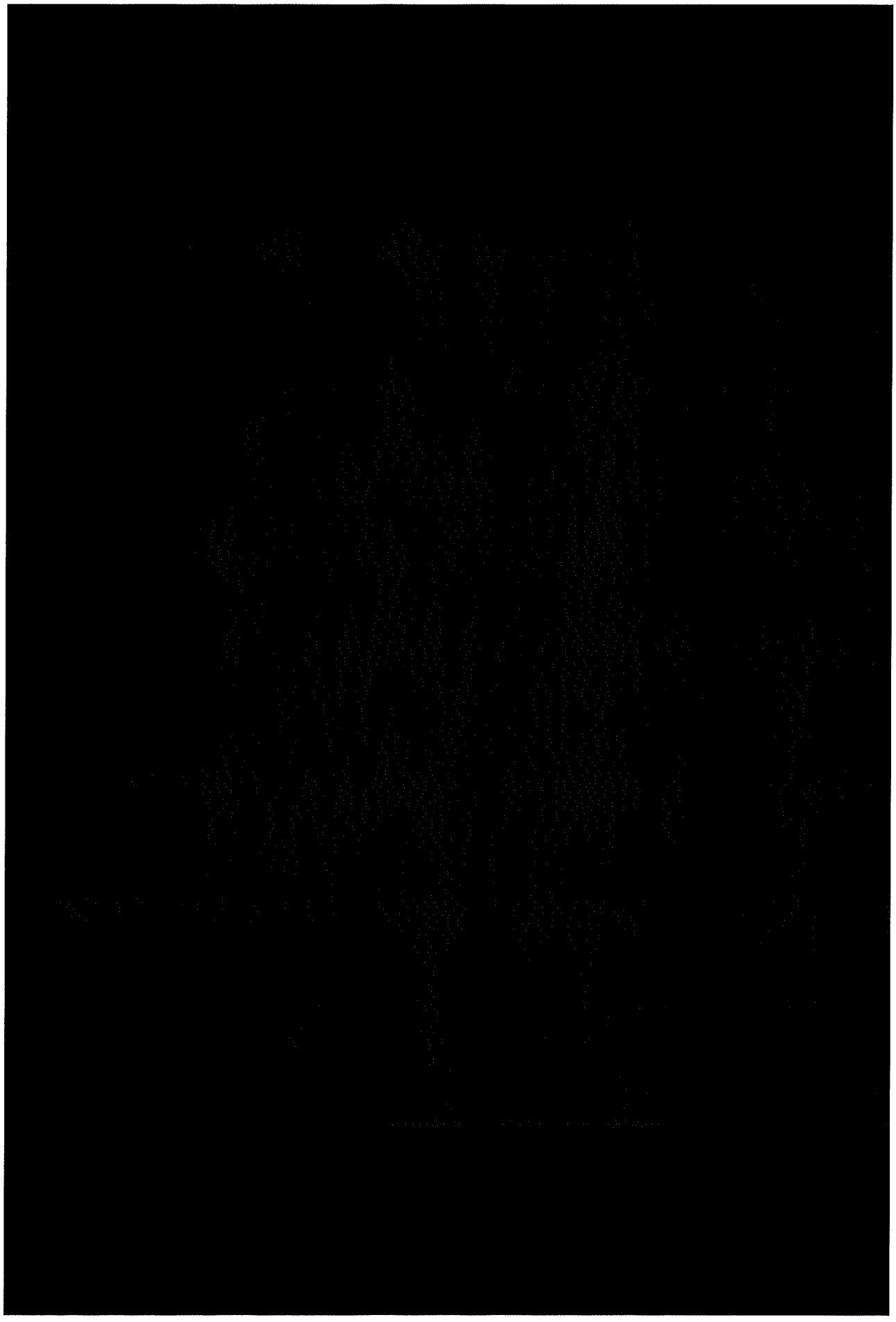




2.3.3 Palm vein counter-spoofing

Considering state of art, the most popular are the texture based approach that consists of texture analysis techniques such: Discrete Cosine Transform (DCT), Local Binary Pattern (LBP), Histogram of Gradient (HOG), Discrete Wavelet Transform (DWT) and the number of filters. The common method in anti-spoofing is to first acquire the image of the spoofed image, extract the image features using one of the above techniques and then use trained SVM (Support Vector Machines) classifier to classify whether the image is real of fake.





2.4 Standards Overview

Currently ongoing at both the national and international levels, fingerprints and biometrics standards development is an essential element especially in fingerprint recognition because of the vast variety of algorithms and sensors available on the market. Interoperability is a crucial aspect of product implementation, meaning that images obtained by one device must be capable of being interpreted by a computer using another device.

In light of the absence of a closed definition, biometric spoofing is widely understood as the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting to the sensor a synthetic forged version (i.e., artefact) of the original biometric trait. Such attacks, also referred to in some cases as direct attacks fall within the larger category "presentation attacks", defined in the latest draft of the ISO/IEC 30107 standard as "presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system".

Fingerprint recognition is the most standardised technology in the field of biometrics, as it has been on the market for decades. As there is a significant number of sensors and algorithms, there have been users' requests for the interoperability between different products. This means that the fingerprint images generated by one solution can be also used by various algorithms.

Certification provides assurance that biometric collection solutions meet or exceed minimum FBI-defined interoperability standards and work with the Integrated Automated Fingerprint Information System (IAFIS) and other AFIS database systems used around the world. Adherence to these standards ensures that images retained by the system are of a specific, high quality and support all phases of identification for both fingerprint experts and IAFIS. Certification is pursued by the relevant equipment vendors to comply with the following standards:

- **FBI IAFIS IQS CJIS-RS-0010 (V7) Appendix F compliance:**

[redacted]

- **PIV-071006:**

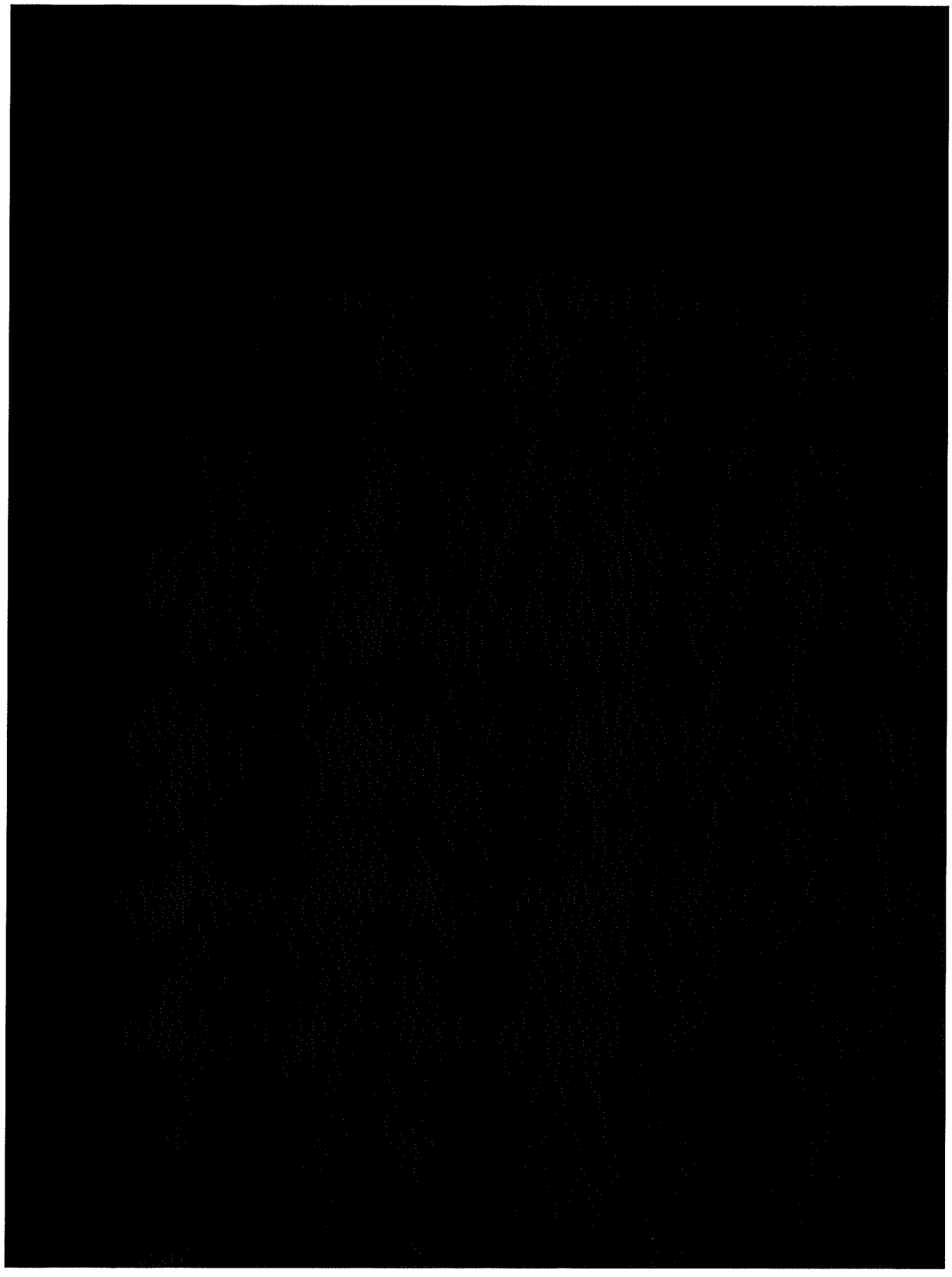
[redacted]

- **ISO/IEC FCD 19794-4 Finger Image Based Interchange Format:**

[redacted]

- **ANSI/NIST-ITL 1-2007; ANSI/NIST-ITL 1-2000; ANSI/NIST-ITL 1-2000:**

[redacted]



3 Biometric Sensors

3.1 Introduction

Biometric technologies perform measurements and analysis based on statistics of individual's physiological and behavioural characteristics. Biometric features are proven to be unique for each person and they can successfully serve as a measure to verify one's identity.

Biometric solutions can be divided into two main categories:

- Physiological analysis: The unique structure of a body or body part
- Behavioural characteristics: The behaviour of a person.

There are various biometric technologies for ID verification based on physiological characteristics, which include DNA, face recognition, fingerprint authentication, palm vein, iris, retina etc. Behavioural solutions, on the other hand, measure the unique behaviour of a person, such as walking, typing, gestures, speech etc.

Biometric systems have the following main parts:

- A biometric reader device.
- A central and local software that converts a scanned biometric template into digital data and carries out the matching.
- The biometric database, which contains all biometric templates.

Biometric authentication systems can be tested and compared in the following three ways:

- Comparing different algorithms, a basis database containing the enrolled biometric templates (e.g. images) will be created with an independent reader. All technologies, which will be compared use the basis database with the same input, where the collected templates might not be optimal for each algorithm just like the size of the database. In case of face recognition or fingerprint authentication, the requirements for size, quality of the images are not the same for all technologies, therefore different solutions use the database with different efficiency. Since all algorithms use the same database as origin, the results can be reproduced continuously and the effectiveness of algorithms can be compared.
- When applying a scenario test, the complete solution package will be tested similarly to a real use. To be able to compare different systems, it is important to create similar conditions for all solutions. Also the expected results have to be planned with great care. Otherwise, it is difficult to reproduce the results. A large scale database can help in this procedure.
- While using an operational test, the system is operated similarly to real conditions with the end users. However, through the application of this method, the reproduction of the results might be difficult, as too many factors can change from time to time.

The most important factor, however, when comparing different biometric technologies is the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The FAR represents a security risk, while FRR means only an inconvenience. When discussing the false acceptance or false rejection, the following terms have to be defined:

- Positive matching means that the person is known by the biometric system and is already enrolled in the system. This stands for 1:n identification.
- Negative matching means that the person is not known by the biometric system. Either a condition influences authentication process or the person's data are not stored in the database.

- Verified matching result means that the system receives additional information from the person before authentication. Therefore the user ID is known and the system has to carry out only a matching between the previously enrolled template and the capture template (1:1 verification).
- FAR shows the calculated number of events, when the biometric system mistakenly accepts a matching request, which is security risk.
- FRR shows when a person, who is enrolled in the system, is rejected by mistake
- Equal Error Rate (EER) is the cross of FAR and FRR.

Considering the above mentioned factors, different biometric solutions can be compared based on the combination of FAR and FRR. In case of biometric access control systems, the following additional terms are used:

- False Match Rate (FMR) means the authentication system's probability to make a positive matching when the biometric template is mixed with other person's biometric ID multiple times.
- False Non Match Rate (FNMR) means the number of events, where the biometric authentication system mistakenly rejects the captured template multiple times even after several enrolments.

FAR/FRR and FMR/FNMR are not identical terms as the latter terms mean that multiple authentication attempts have been carried out. FAR/FRR describes the basic acceptance procedure, which can have following failures:

- The rate of low quality biometric templates, which makes the secure authentication impossible as the security score of the matching would be too low,
- The rate of false biometric sample, where the biometric templates increase significantly the FRR due to the low security score.

Comparing biometric technologies is difficult as most solution providers have not been certified by independent laboratories but their figures have been defined by companies themselves or this information are not provided at all. The purpose of this review is to give a detailed market overview concerning the biometric technologies to highlight the possibilities of actual technologies.

3.2 Fingerprint Sensors

3.2.1 Background knowledge

Fingerprint recognition means the authentication and matching of two fingerprint templates. This technology is one of the most widely spread solutions in the world, since it is easy to deploy, use and, besides face recognition, it is the best solution for law enforcement agencies. What is important to take into account is that, like all biometric systems, it has two different parts: the sensor that captures the biometric print (in this case the fingerprints) and the algorithm that does the actual match.

3.2.1.1 Technologies for extracting fingerprints - sensor technologies

As stated previously, a fingerprint biometric module consists of two main parts: the sensors (hardware) and the matching algorithms (software).

In the framework of this Deliverable, the analysis that follows concentrates on the technologies used for the hardware i.e. the fingerprints sensors, readers and scanners that are already in use at the BCPs and /or that are available on the market.

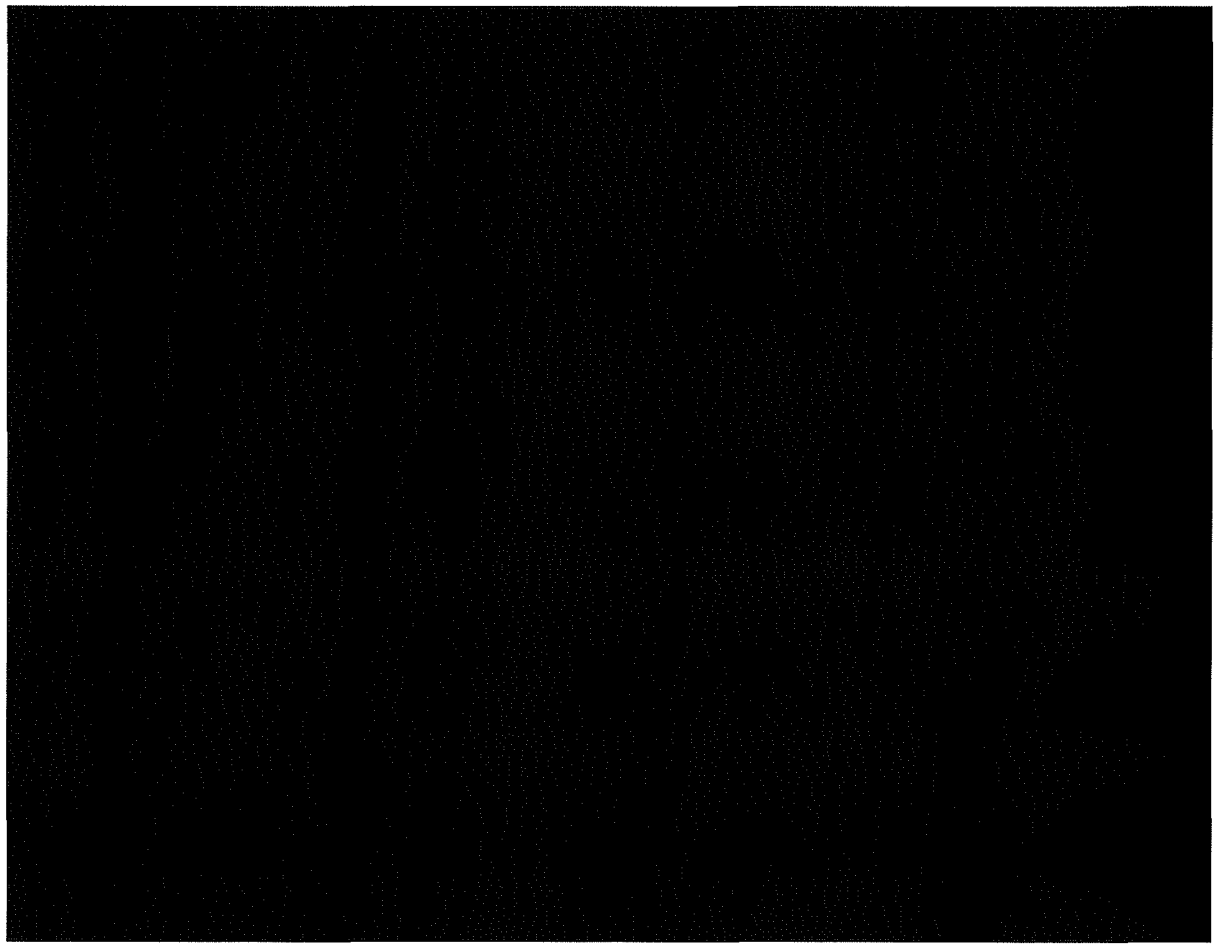
Concerning the corresponding fingerprints matching algorithms, it should be noted that the respective analysis will be presented in detail in the Deliverable D3.2 that follows. However, in this section, the main aspects of the relevant algorithms will be presented to facilitate the reader in order to have an adequate overview of the overall module at this point.

Fingerprint readers technologies

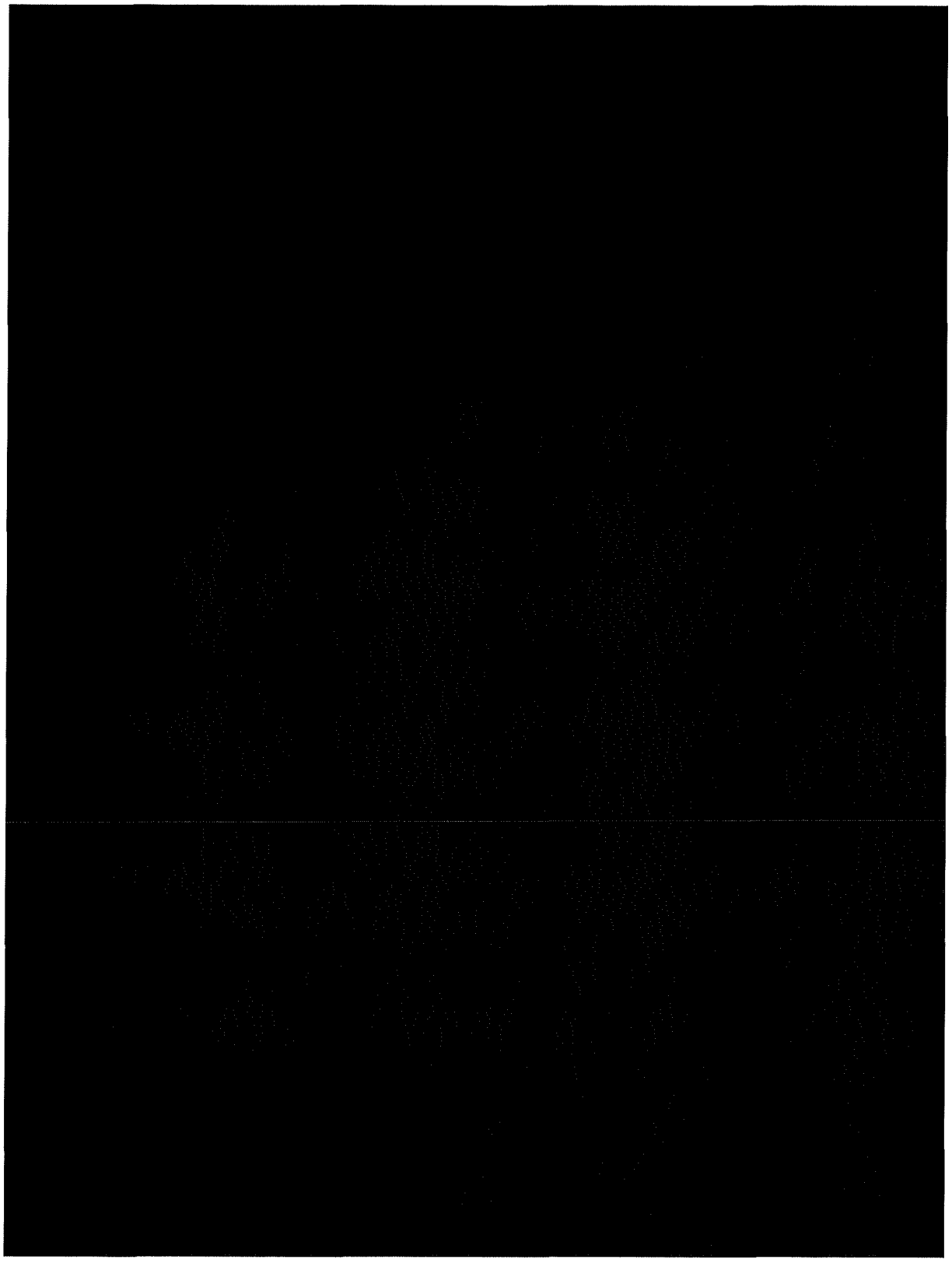
The fingerprint reader recognizes the individual pattern in the fingerprint by various methods. After taking the image, it will be digitalized by a solution, which is later used for biometric authentication, either as BET (Biometric Enrol Template) or BCT (Biometric Capture Template).

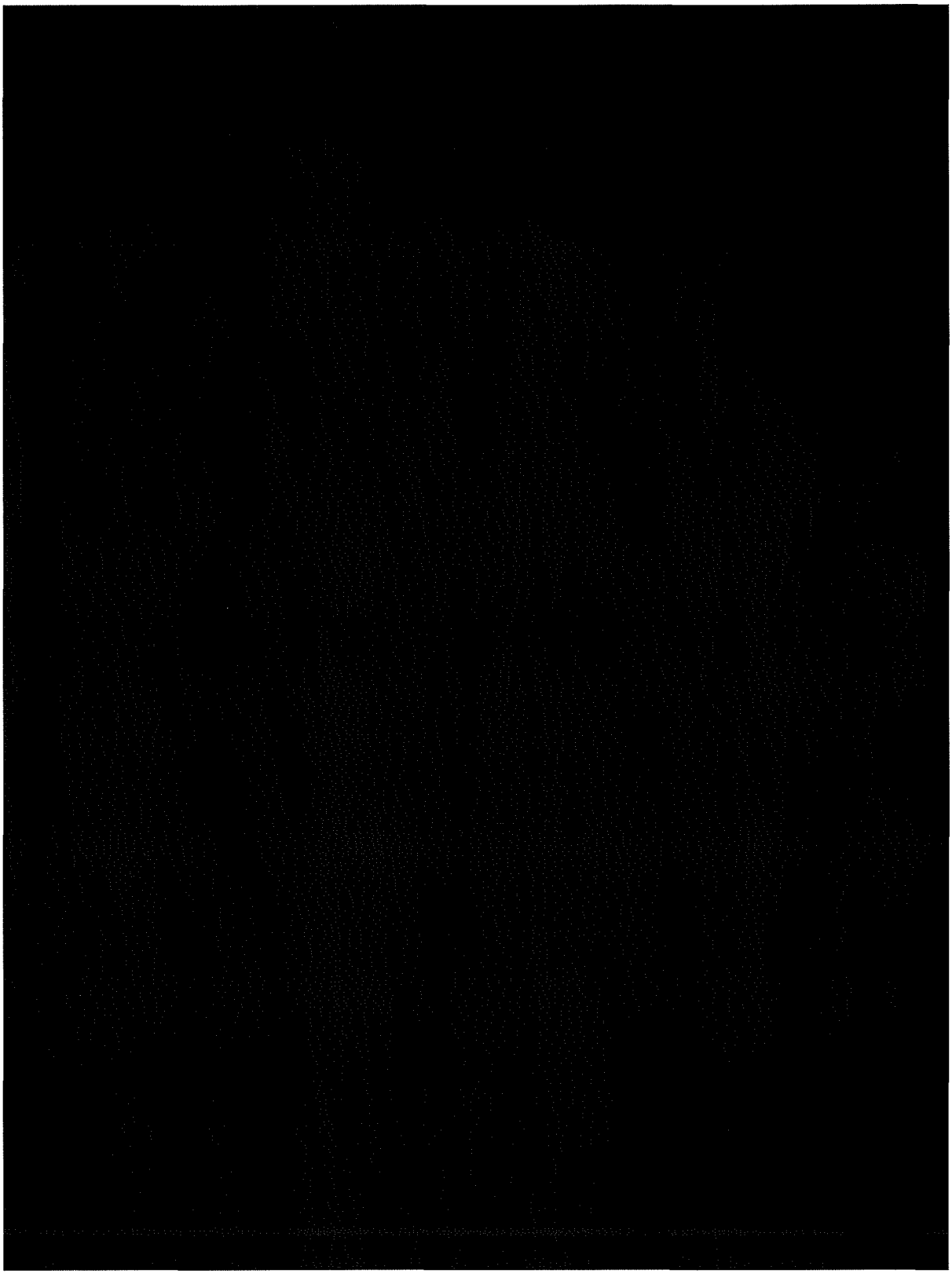
Two are the main technologies of fingerprint sensors that are most commonly used in commercial systems: the optical and the capacitive ones.

In the following a summary of the current technologies that are used for fingerprint reading is given (taken from **National Science and Technology Council (NSTC) - Committees of Technology and Homeland and National Security reports**[9] and also from 360Biometrics Hardware Software Consulting[10] combined with the partners' relevant experience) in order the pros and cons of each technology to be identified.



[9] ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf
[10] http://www.360biometrics.com/faq/fingerprint_scanners.php





3.2.1.2 Algorithms for fingerprint recognition

As stated previously, although, the aspects of the fingerprint matching algorithms will be presented in detail in Deliverable D3.2, certain important features are given herein for facilitating the reader.

All fingerprint matching algorithms compare previously enrolled template with a newly captured fingerprint template for authentication. Various algorithms differ with regard to the technique of biometric matching.

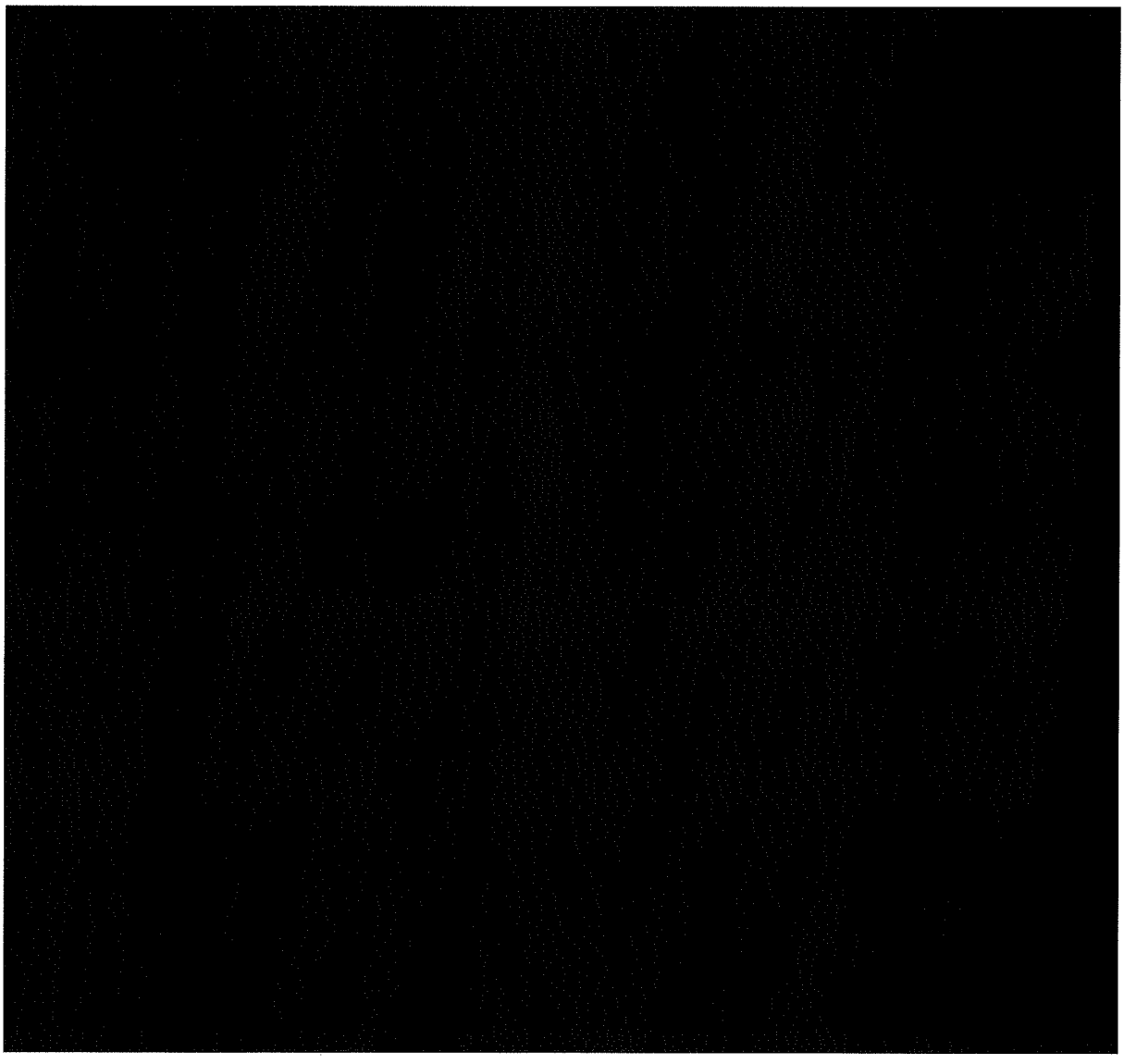
The most common fingerprint authentication algorithms

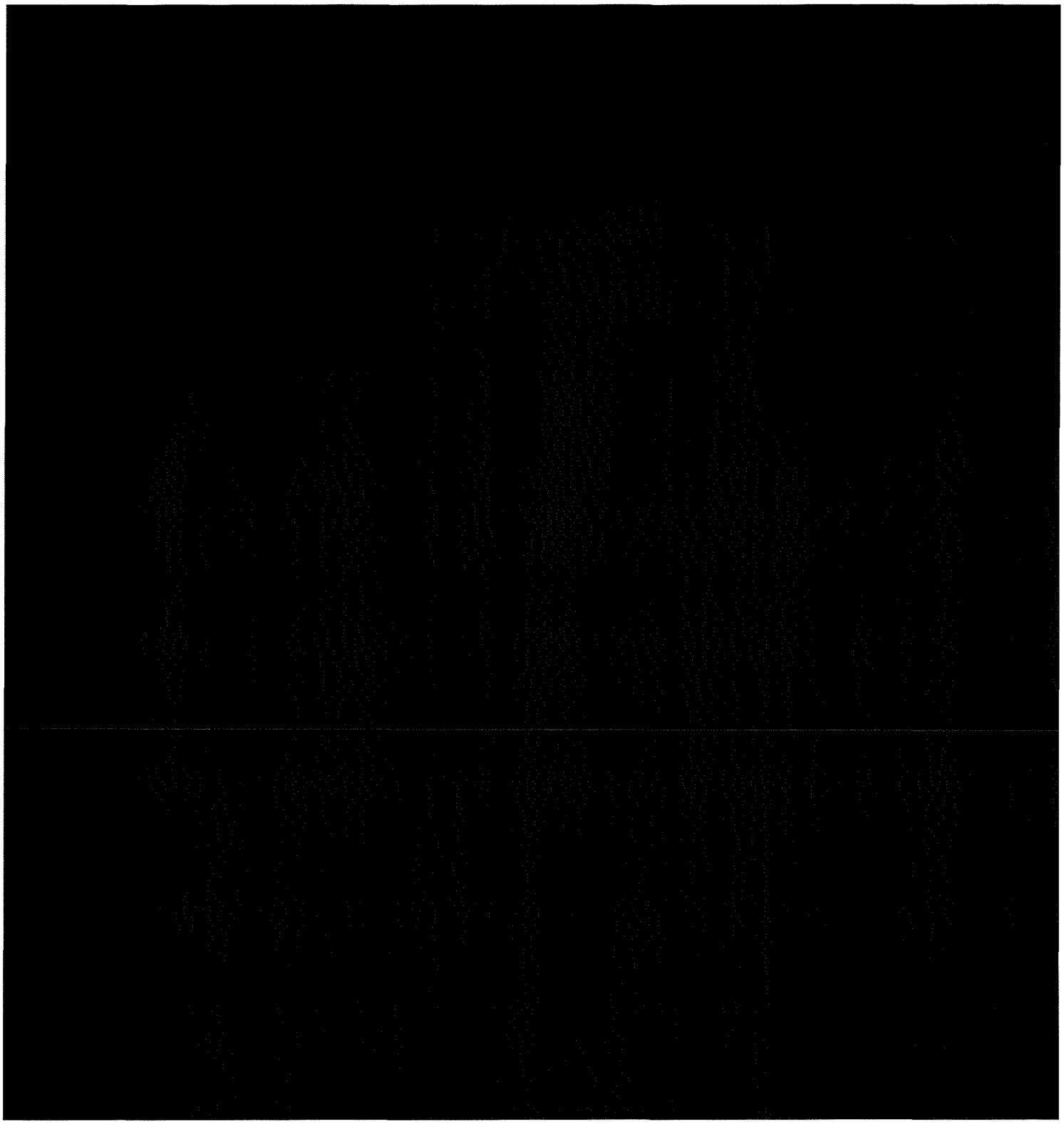
During the biometric authentication, the previously enrolled biometric fingerprint template is matched with the newly captured template. The result of the authentication is a matching score, which determines whether an identification request will be approved or rejected by the system. The Fingerprint recognition system also checks the matching of the grey scale images with the original fingerprint image.

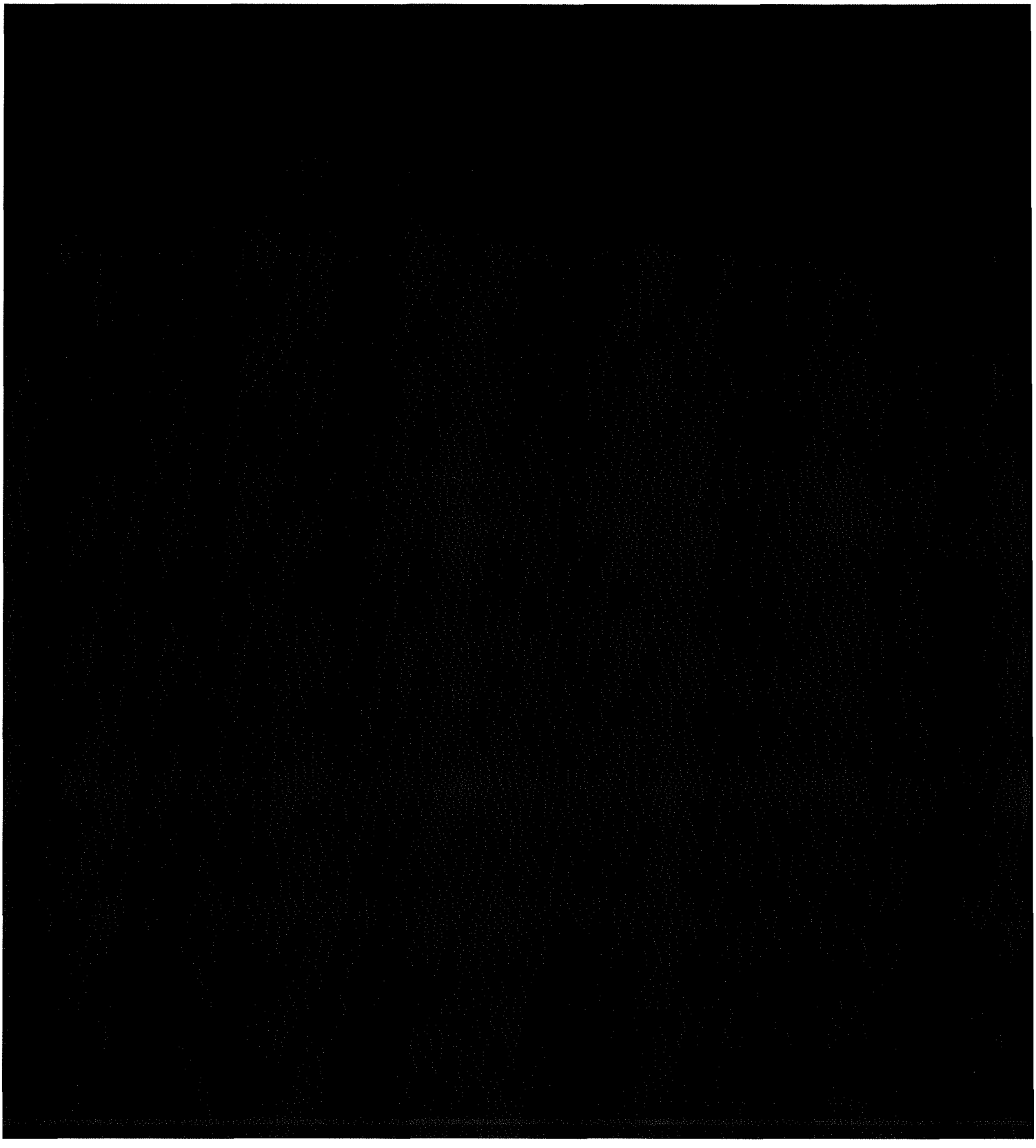
The most significant difficulty in fingerprint recognition is the high variability of fingerprints coming from the same finger. The differences of fingerprints can be caused by the following factors: Displacement of the finger, Partial overlapping, Dirty or injured skin surface, Dirty sensor surface, Light conditions, and the way the finger is pushed against the sensor surface.

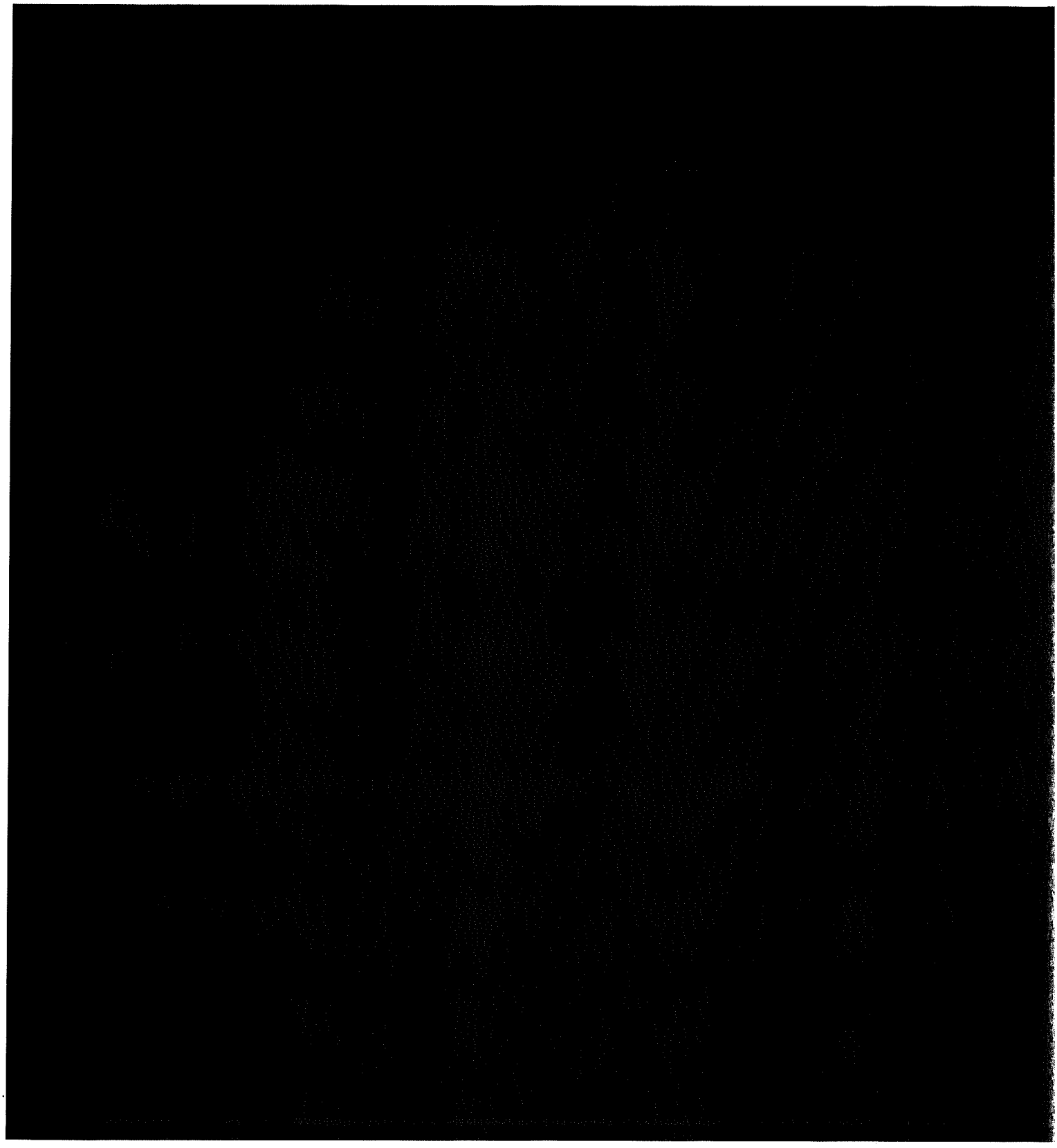
The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching.

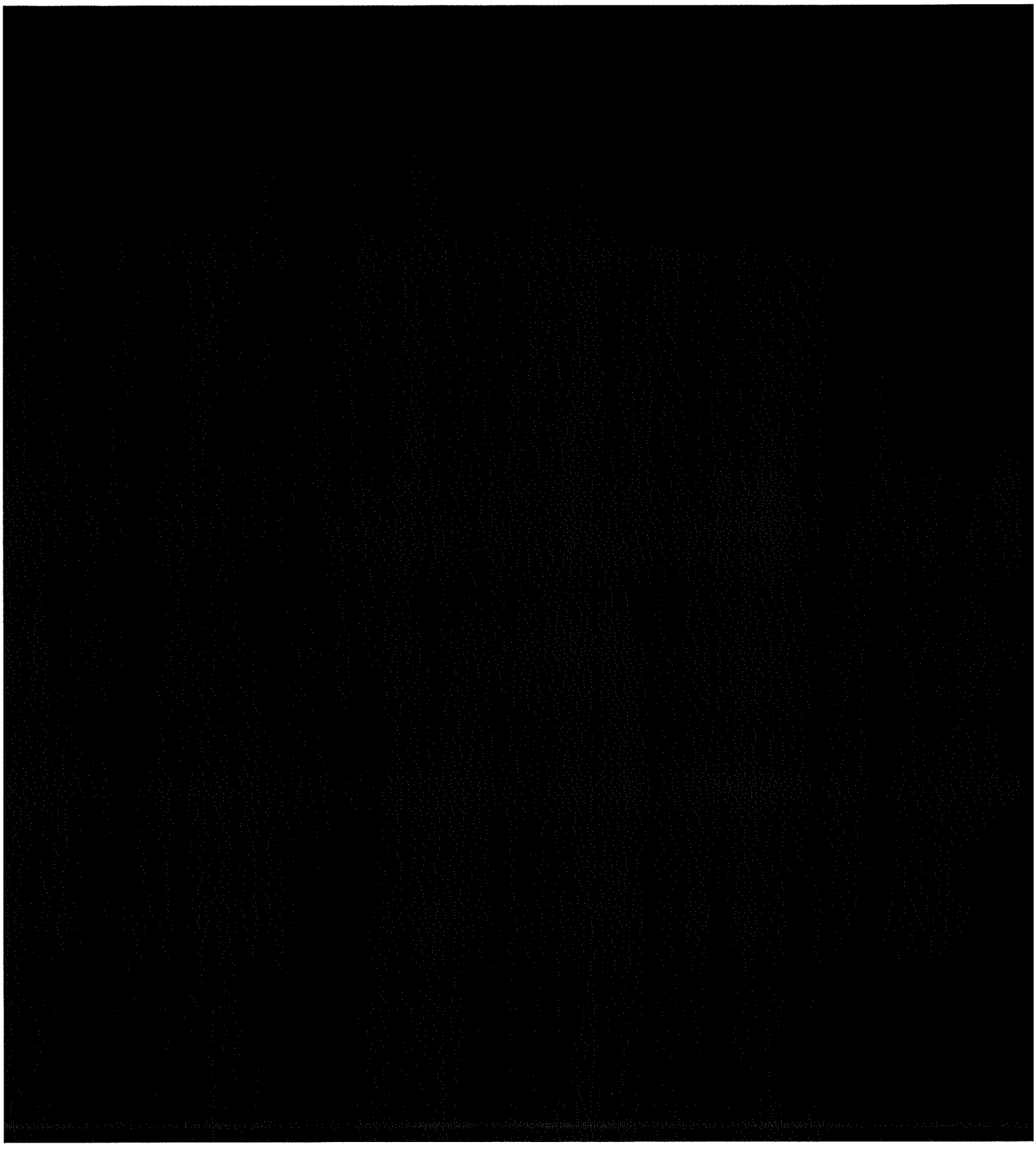
- ***Pattern matching:*** it simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching, relies on the minutiae points described above, specifically the location and direction of each point. Relevant differentiations include **Ridge feature based and Correlation based**. The correlation based authentication requires high computing power. Therefore, only a part of the image will be used for matching.
- ***Minutiae based***: The minutiae based matching is the most widespread technology among fingerprint reading technologies. The fingerprint will be converted into a set of minutiae points, where their position determines the template itself. The positions of the minutiae points of the enrolment and the capture template will be compared to each other. Naturally 100% overlapping cannot be reached, therefore a tolerance rate for the matching will be defined. The only disadvantage of the technology is that, in low quality conditions, the image is not suitable for minutiae matching. Some technologies use a double level matching, first only a small part of the points will be compared and in case of matching, the complete template will be compared.

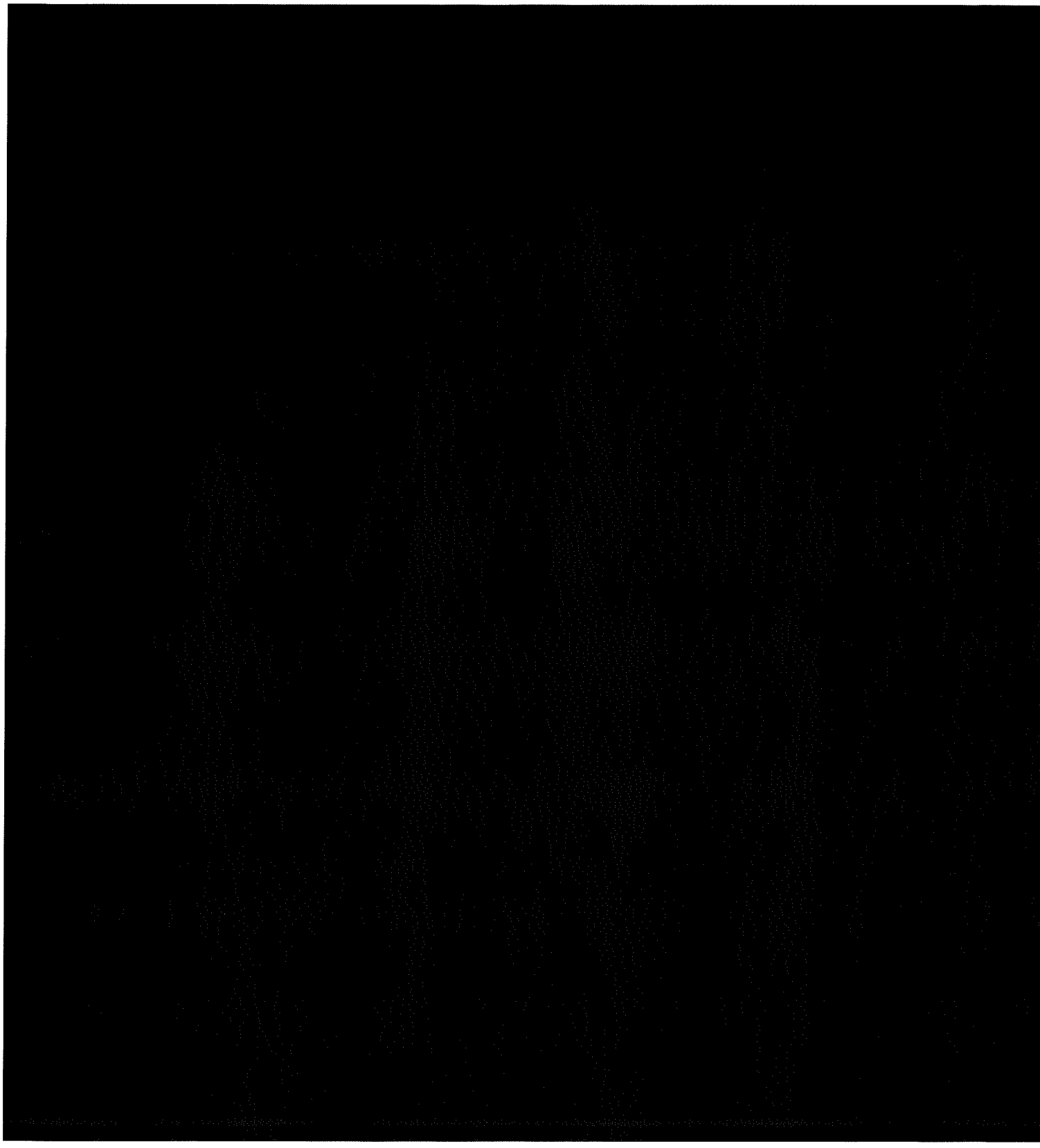


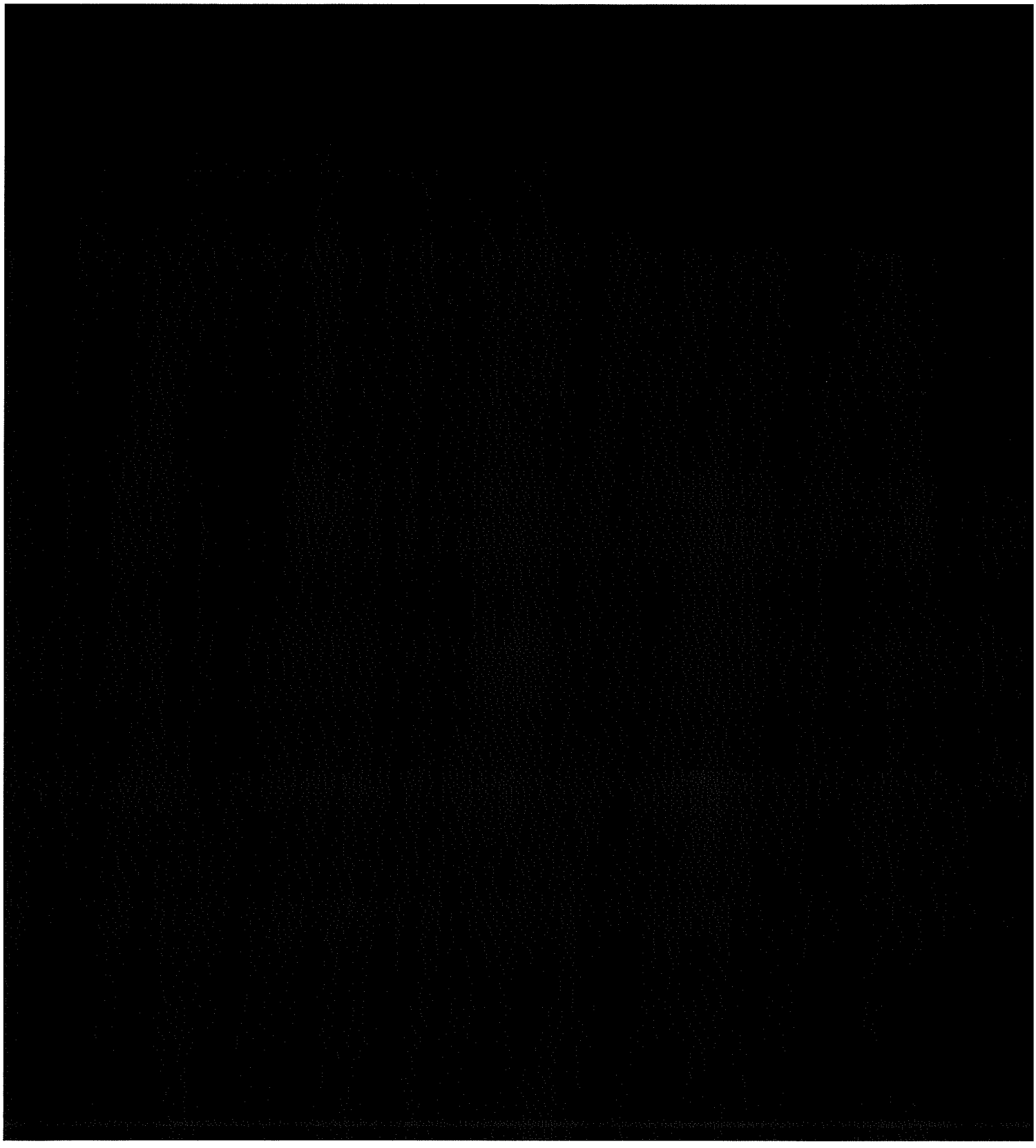


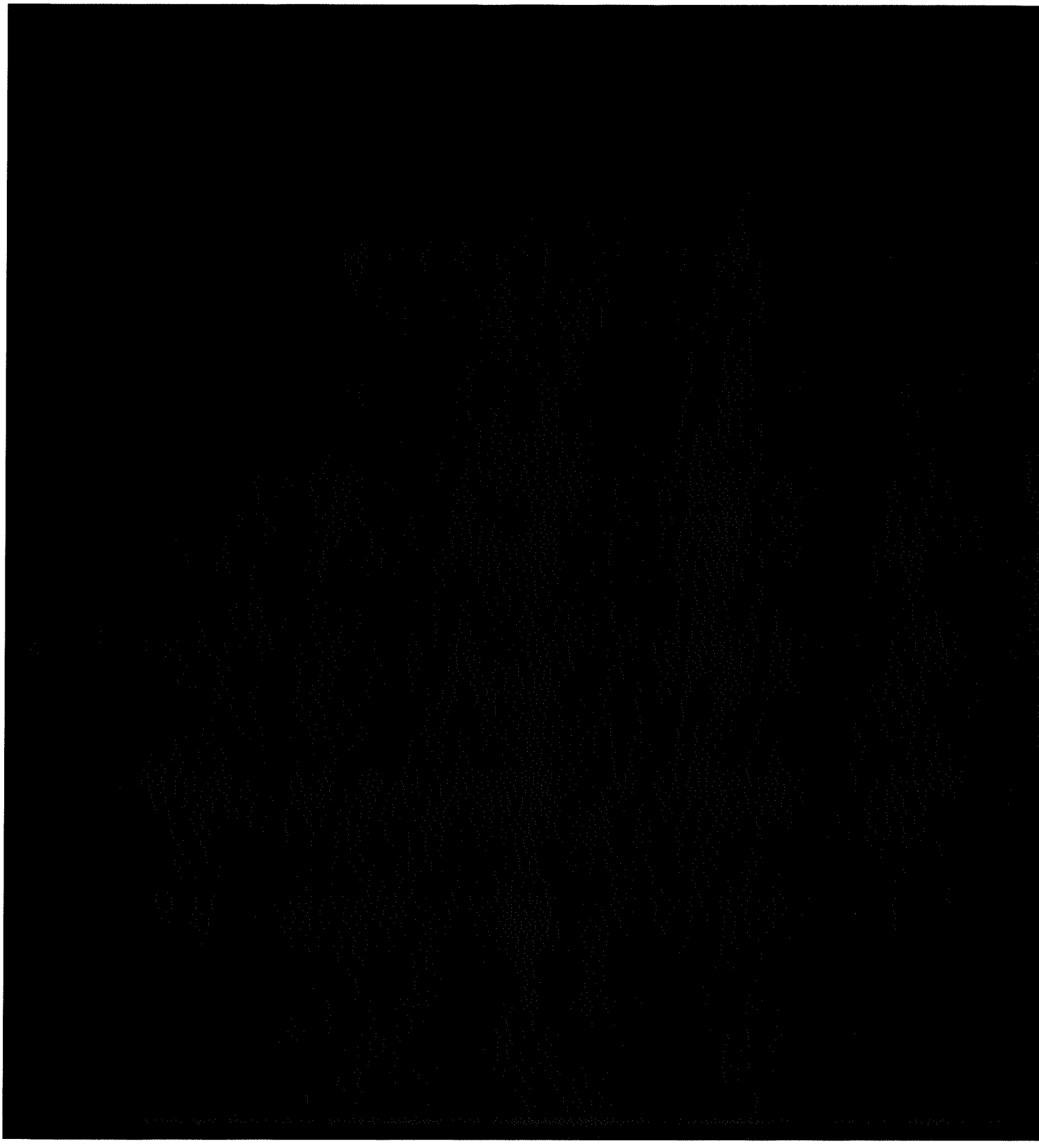












3.3 Palm Vein Sensors

3.3.1 Background knowledge

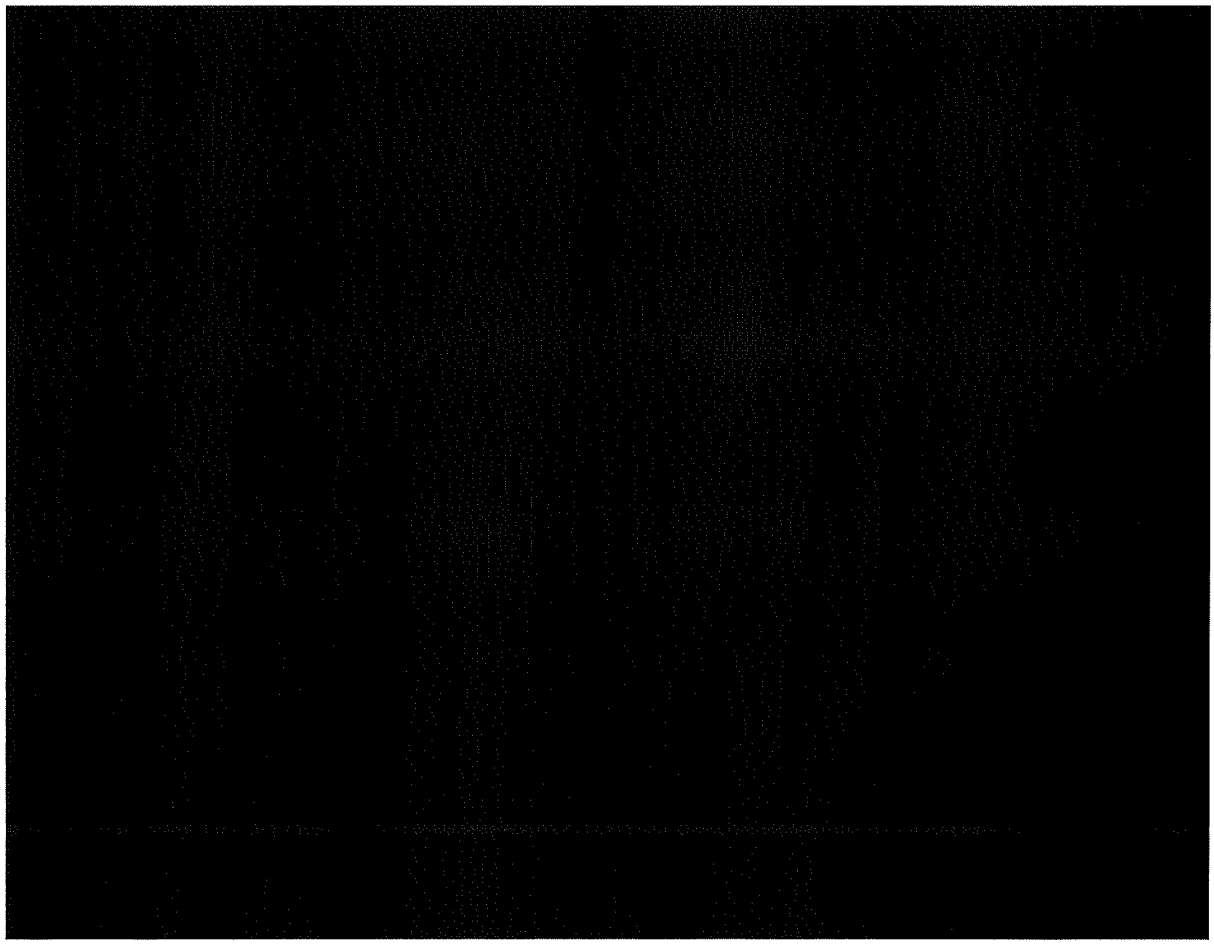
Palm vein readers "read" the vein pattern below the skin by emitting near infrared light. The carbon dioxide reaching blood vessels absorbs the near IR light. As a consequence, the vein structure in the palm becomes visible.

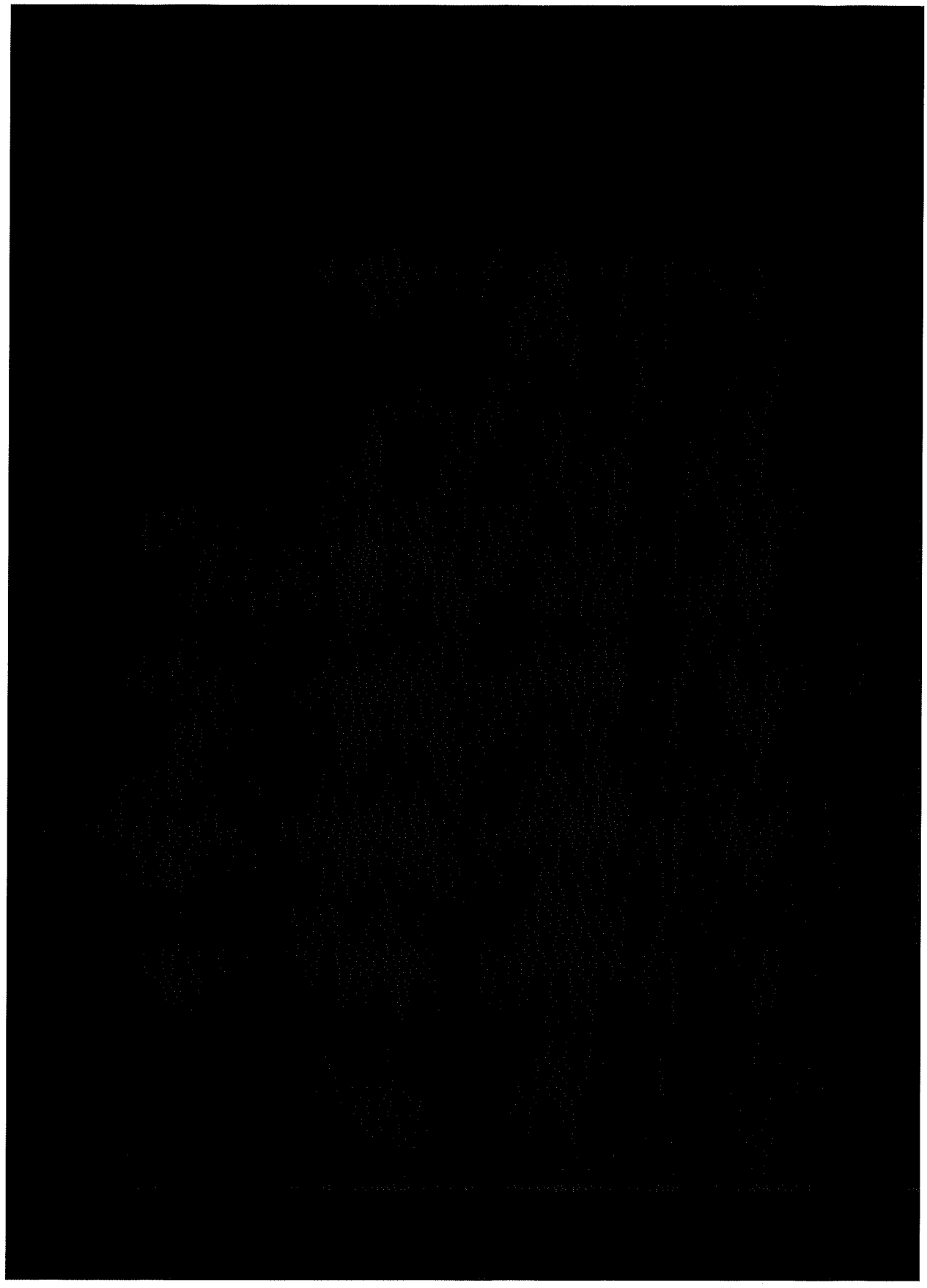
The use of the vein scanners is contactless; the distance of 4-6 centimetres is enough. Common dirt (except oil) or skin surface injuries do not affect the quality of authentication or the matching score. The solutions is fast, as the authentication takes no more than a second depending on the size of the database. The vein pattern below the skin is one of the most unique biometric factors a human body can have. Therefore, vein recognition technologies are among the most secure solutions.

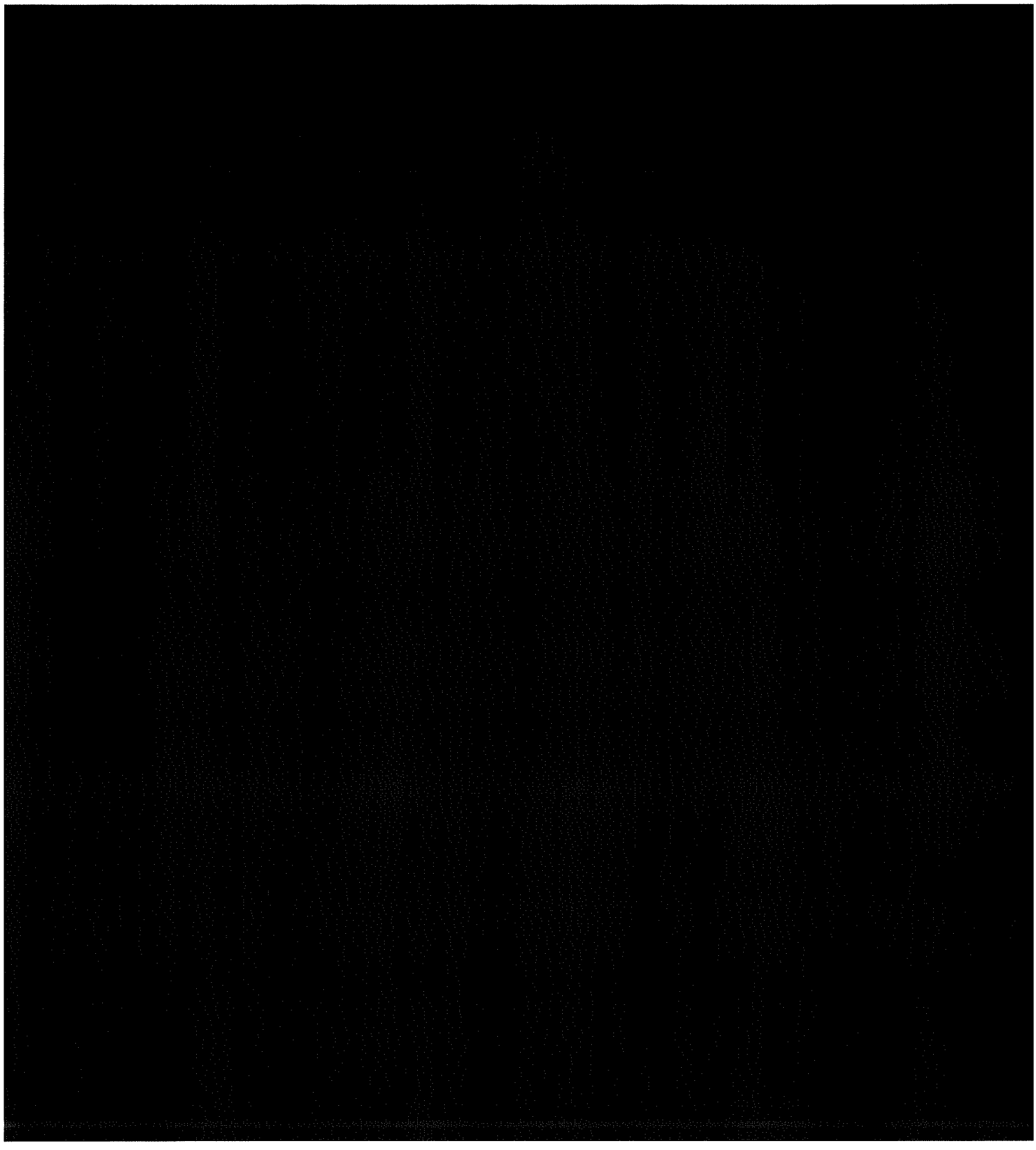
Currently, there seems to be only one company on the market, which produces IR optics and chips for palm vein recognition. This company is specialized in 1:n authentication with large numbers. Fujitsu and BioSec have signed a strategic partnership agreement to elaborate together on the possibilities of palm vein matching.

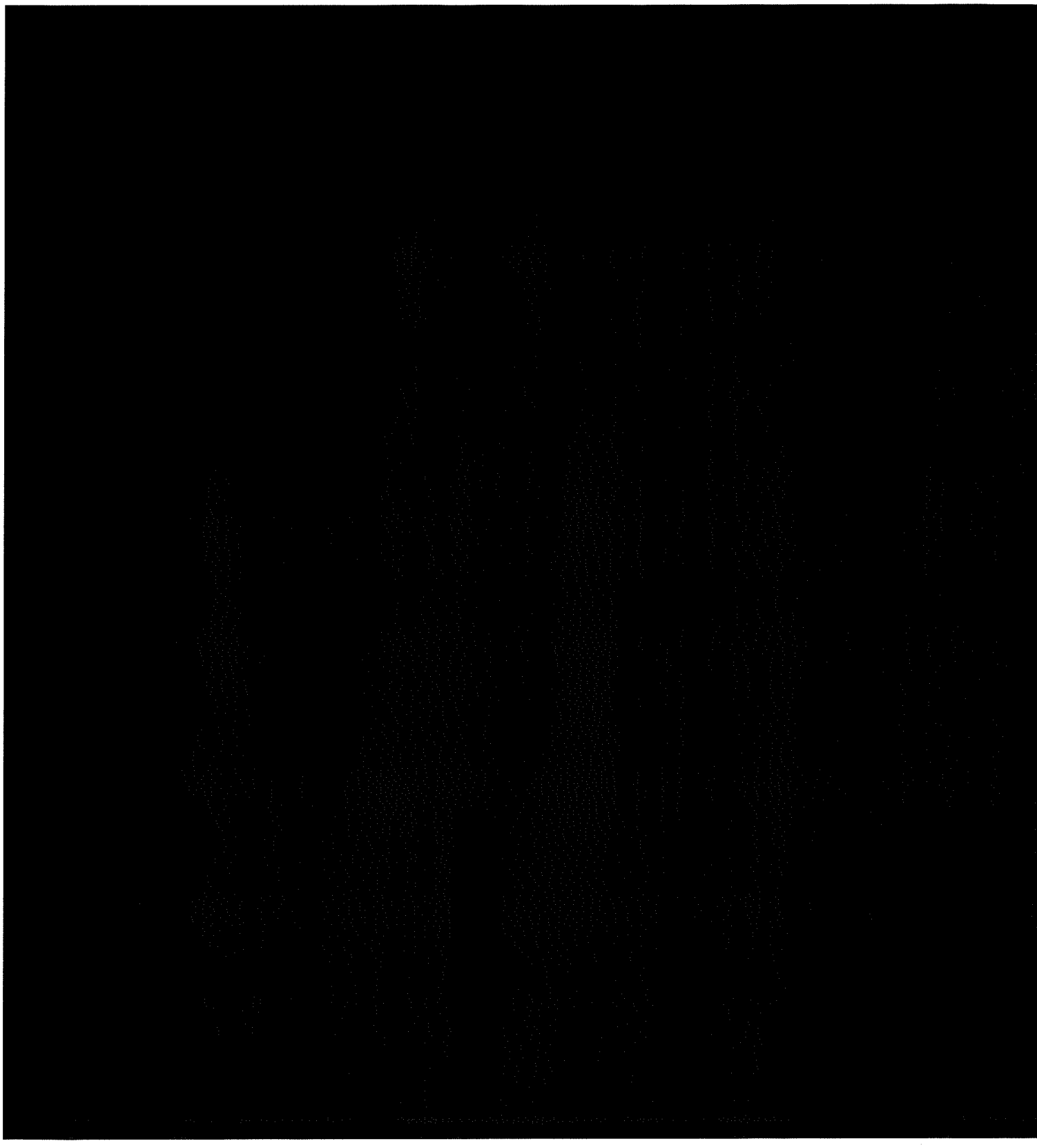
There is no public information of mathematic approaches for palm vein recognition, as this is the latest biometric technology. Therefore, the mathematic algorithm is the subject of business secret and the algorithm approach is not public yet.

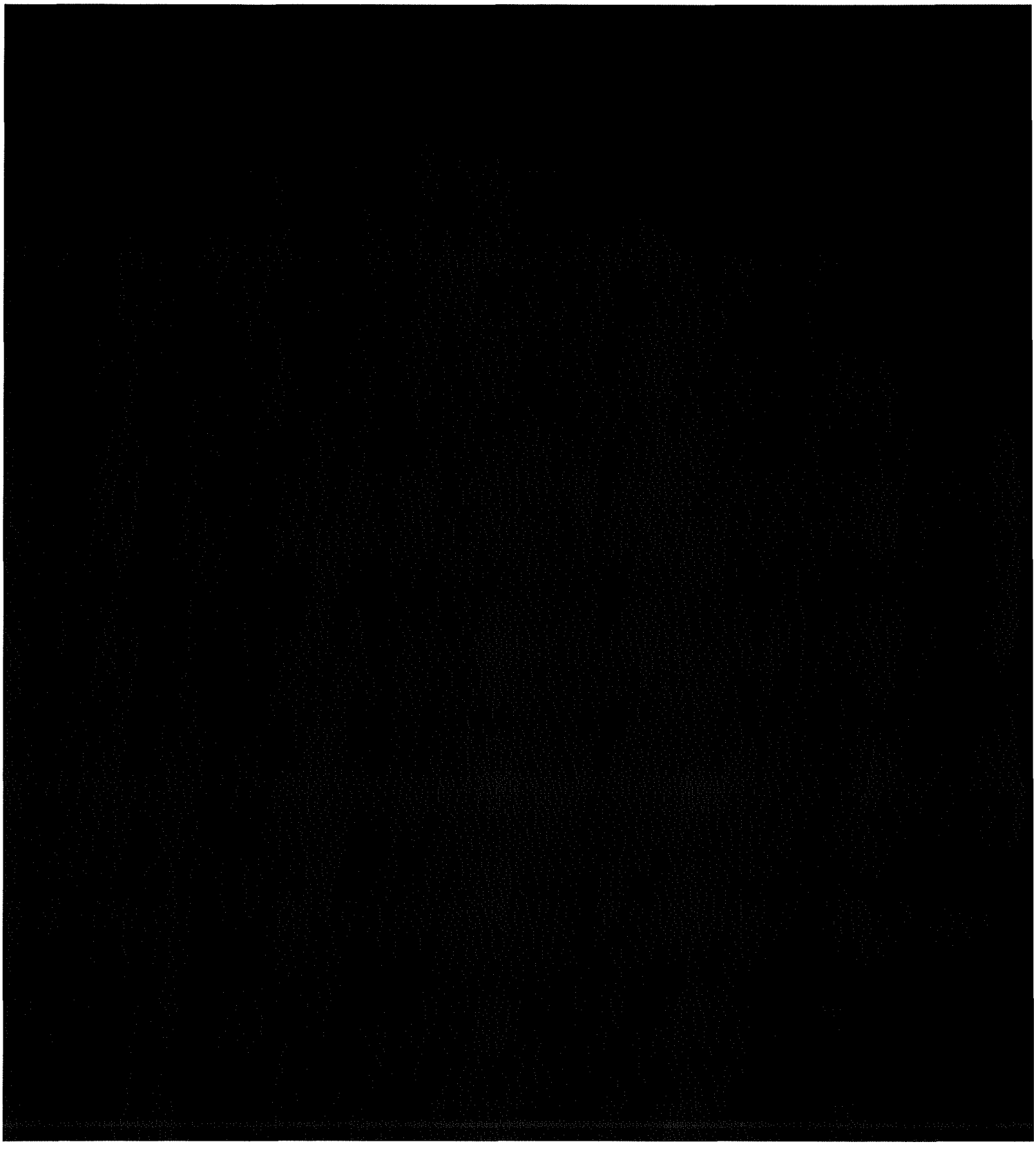
The vein pattern below the skin becomes visible for the IR optic via the absorption of the IR light emission and is based on the complete "vein map". As a consequence, a unique hash code will be created for subsequent matching.











3.4 Face Sensors

3.4.1 Background knowledge

Facial recognition technologies have been developed since early 60's when Woodrow Wilson Bledsoe developed a system that could classify photos of faces by hand using what's known as a RAND tablet, a device used to input horizontal and vertical coordinates on a grid using a stylus that emitted electromagnetic pulses. This mechanism was used to manually record the coordinate locations of various facial features including the eyes, nose, hairline and mouth and store this information in a database. When the system was given a new photo of a subject, it was able to retrieve the image from the database that most closely resemble the subject.

Facial recognition was very limited by the technology available in those times, but thanks to the advances in computer processing capacity, image analysis and the new development of machine learning (or deep learning) the capabilities and results of Facial Recognition Technologies have improved exponentially.

3.4.1.1 Basis information for facial recognition authentication

In Face Recognition there are several definitions that are important to clarify:

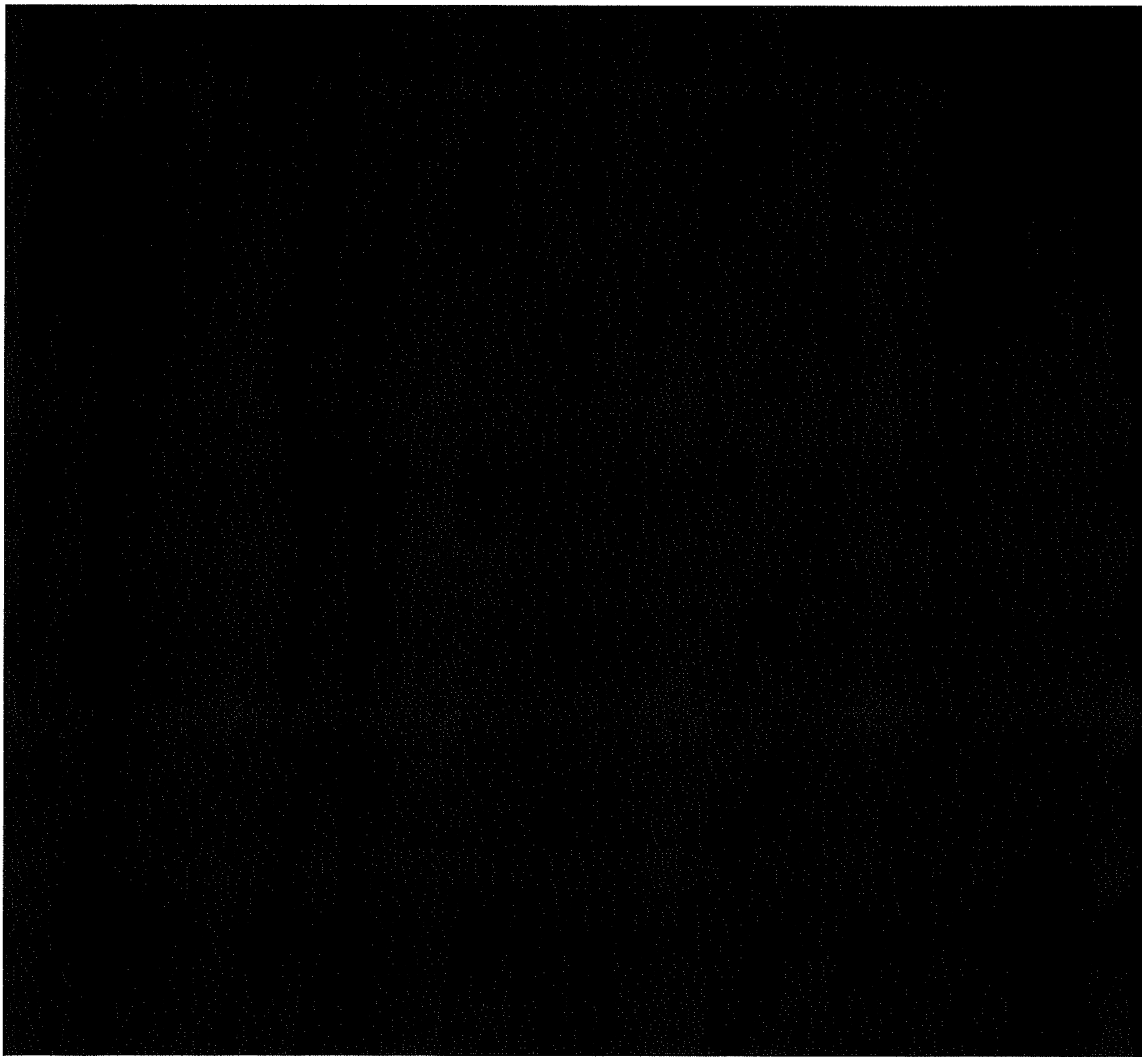
- Face detection: This functionality detects if there is a face (any face) in the image that is being analysed. Depending the algorithm used it could detect several faces in the same image or only one.
- Face recognition: This functionality tries to identify a face already detected within a database of stored faces.
- Validation: In this case the system compares the image with the stored template of a subject in the database to verify if is the same persona (1:1 comparison)
- Identification: The system search the database to see if there is any possible match with the subject in the image (1:N comparison)

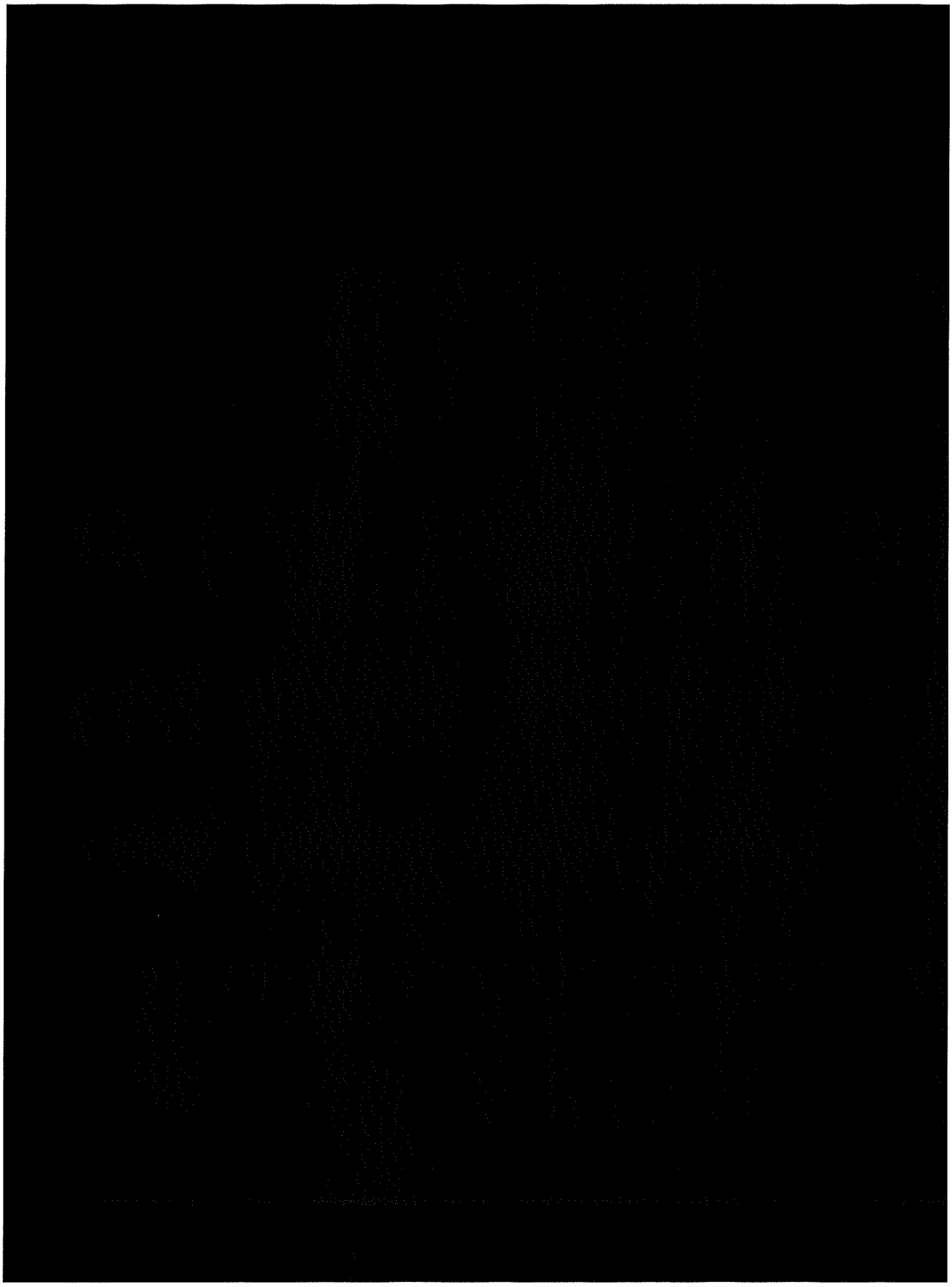
All Facial Recognition systems follow the next steps in order to perform facial recognition:

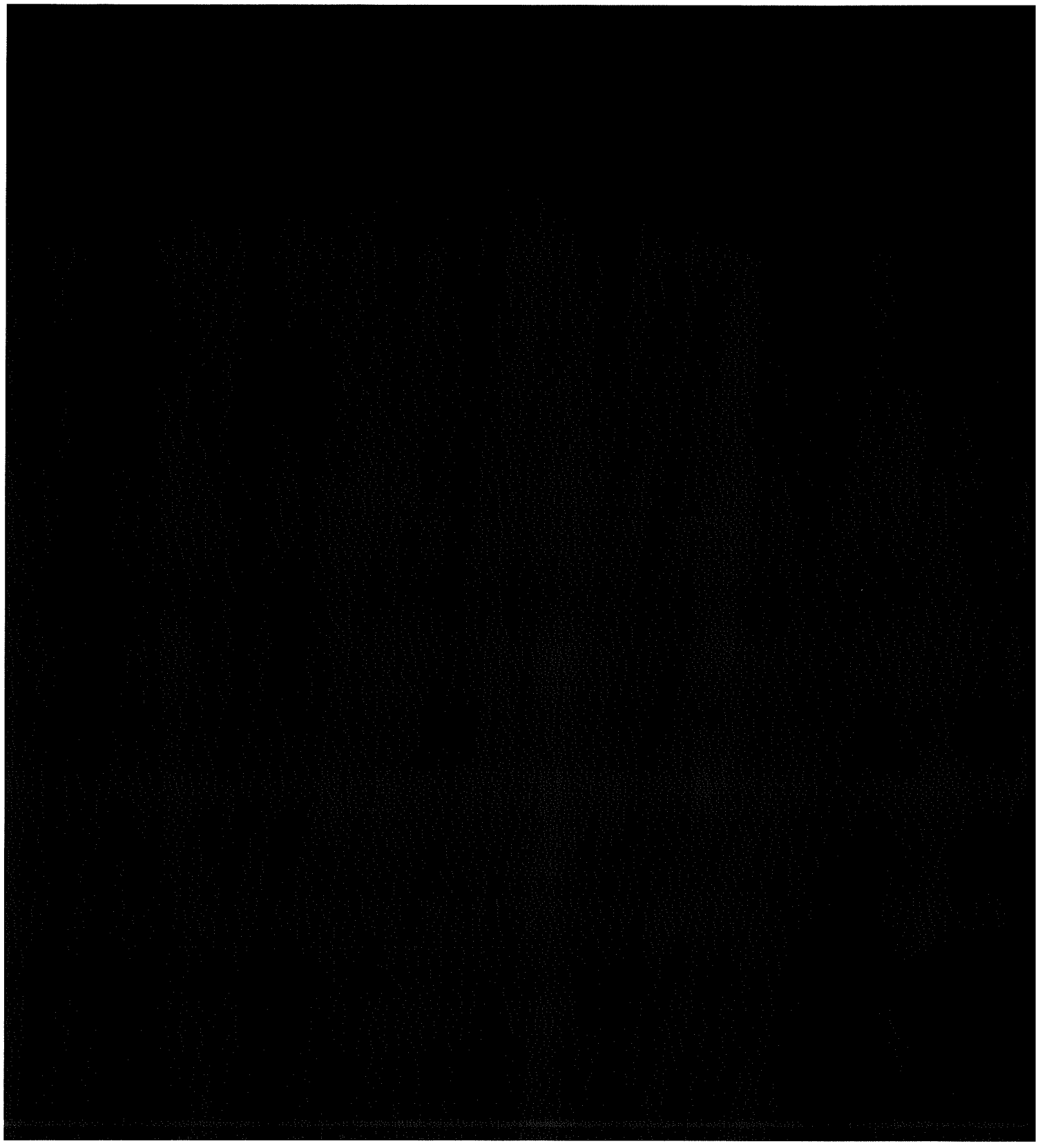
1. A digital camera (hardware) takes an image of the face presented.
2. The system (software) performs Face Detection on the image.
3. When a face has been detected, the geometry will be analysed and the features necessary for identification will be extracted. Each solution provider uses its own approach and algorithms to perform this task.
4. The captured template will be matched with the enrolment template for authentication either in identification or verification mode.
5. As a result of the matching procedure, a score will be defined. The score limits will be defined by each solution provider/developer, which has a direct proportional connection to FAR (False Acceptance Rate) and FRR (False Rejection Rate).

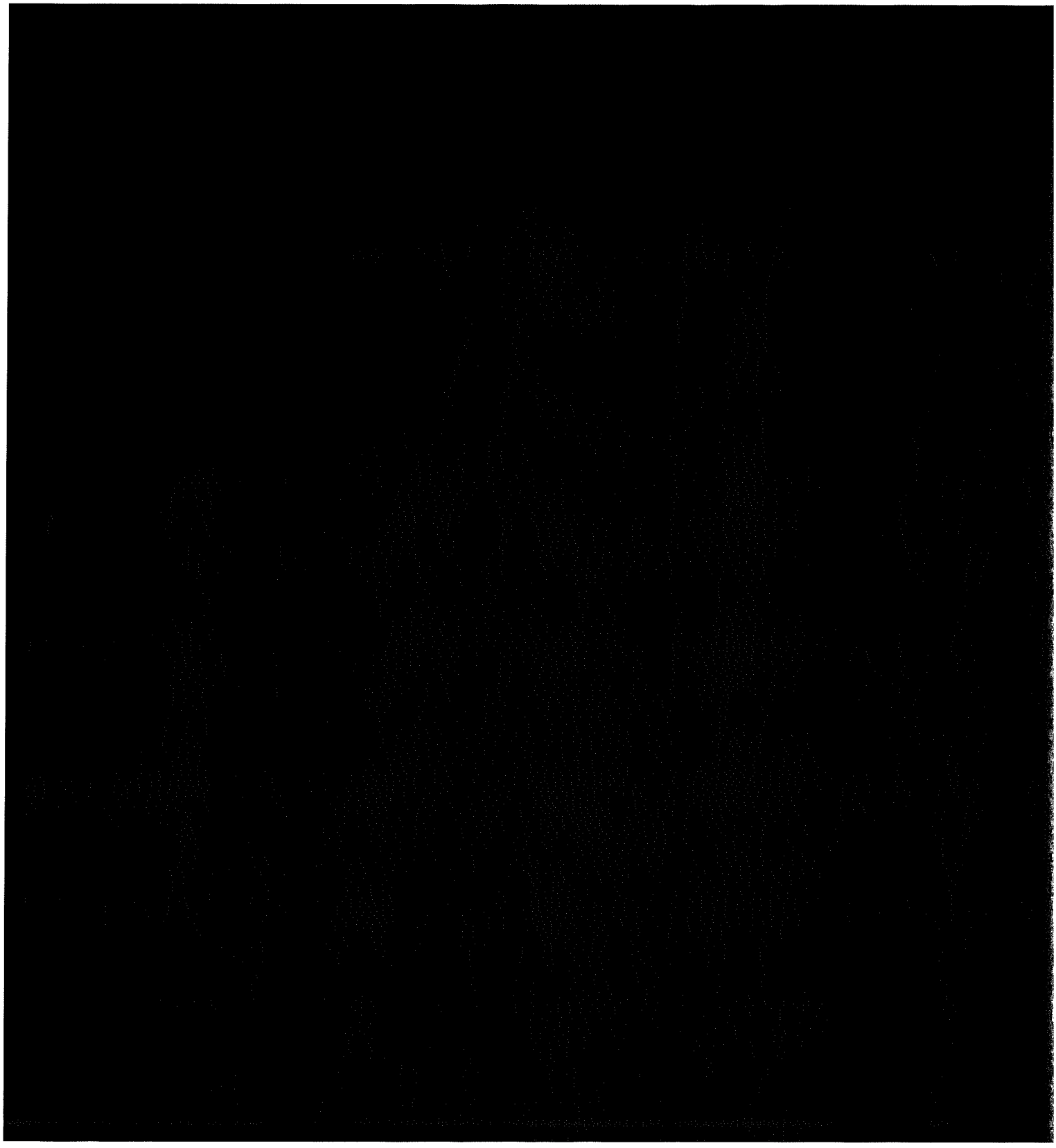
In all the biometric systems the quality of the image capture to compare it with the stored template is important, but in the case of Facial recognition is crucial. During the first years of development of Facial Recognition solutions, the results were very dependent on the quality of the image, the ageing of the subject, the light and shadows in the image, the frontality of the subject and the changes like beards or glasses. However, the new advances in deep learning technologies and the use of GPU computational power have provided to Facial Recognition software developers new tools and capacities to overcome those problems.

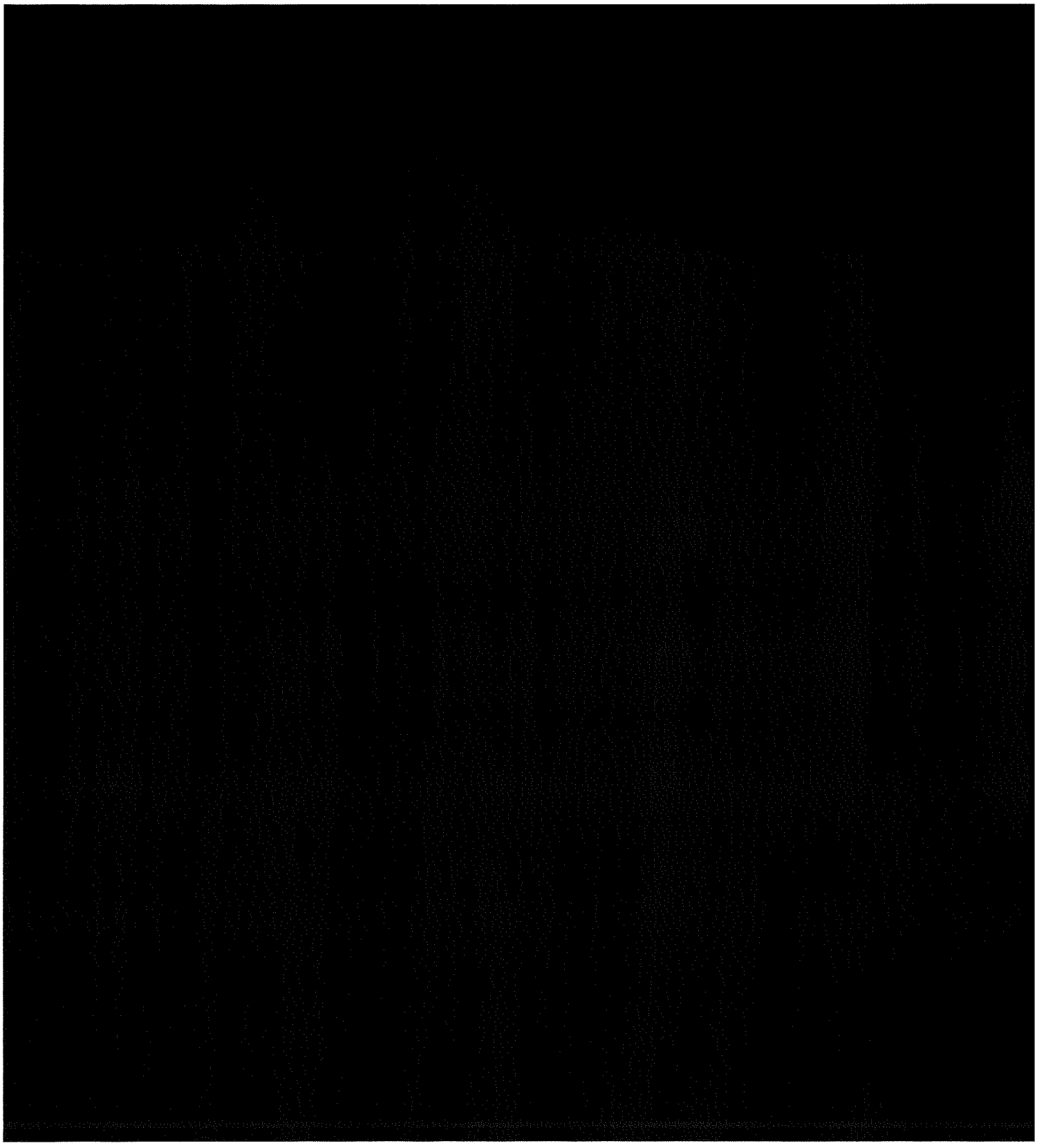
It is important to understand however that even with the most advanced algorithms facial recognition technologies are not going to work properly if the subject in the image is partially covered (big and dark sunglasses, scarf obscuring half the face, etc.), the image is not a near frontal one (the subject shows only half of the face due to camera angle or because is looking to the side) or the light is not right (the subject has a source light to their back, creating shadows in the face); therefore further enhancements are realised for both hardware as well as software components composing the technology.

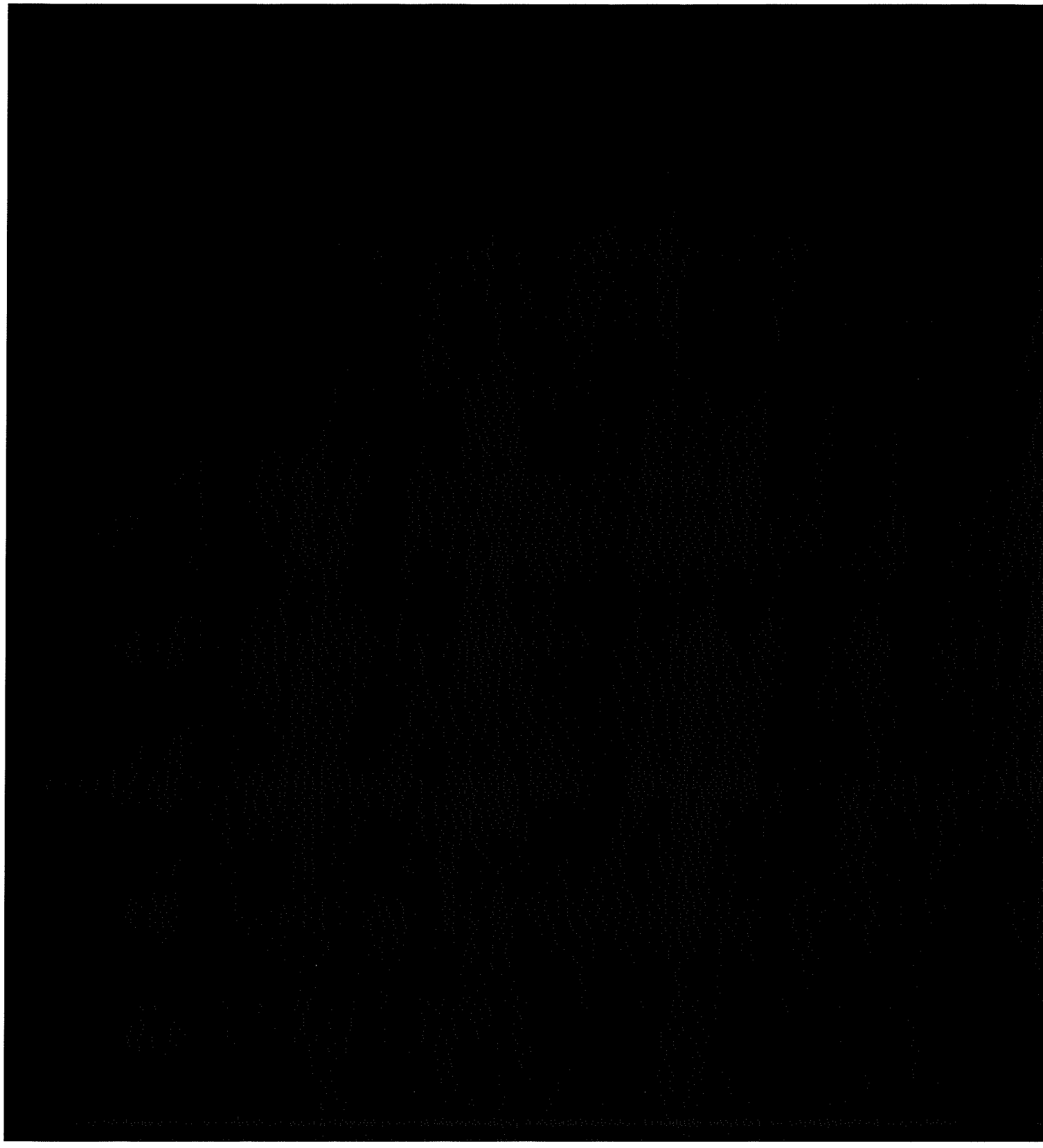


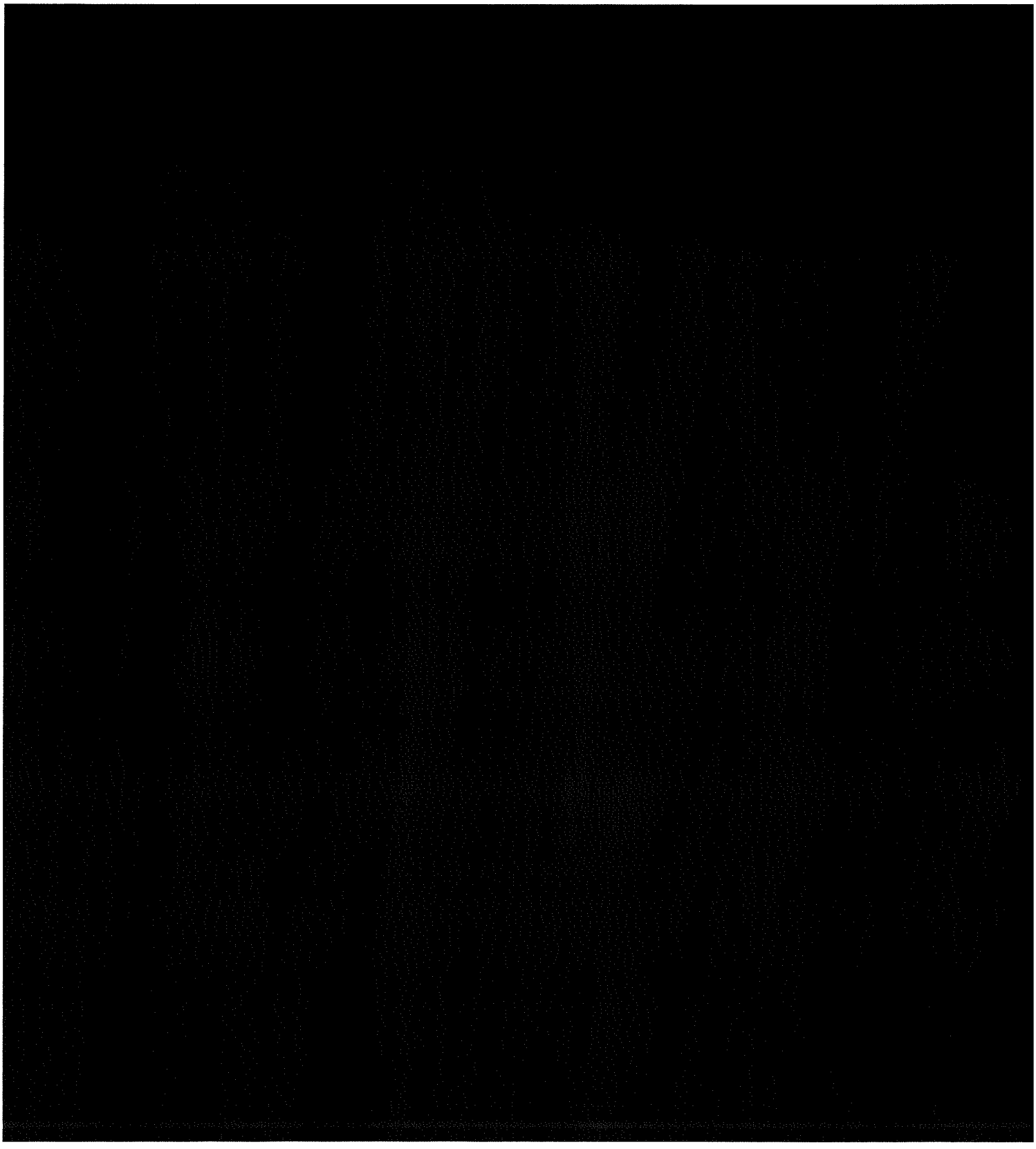


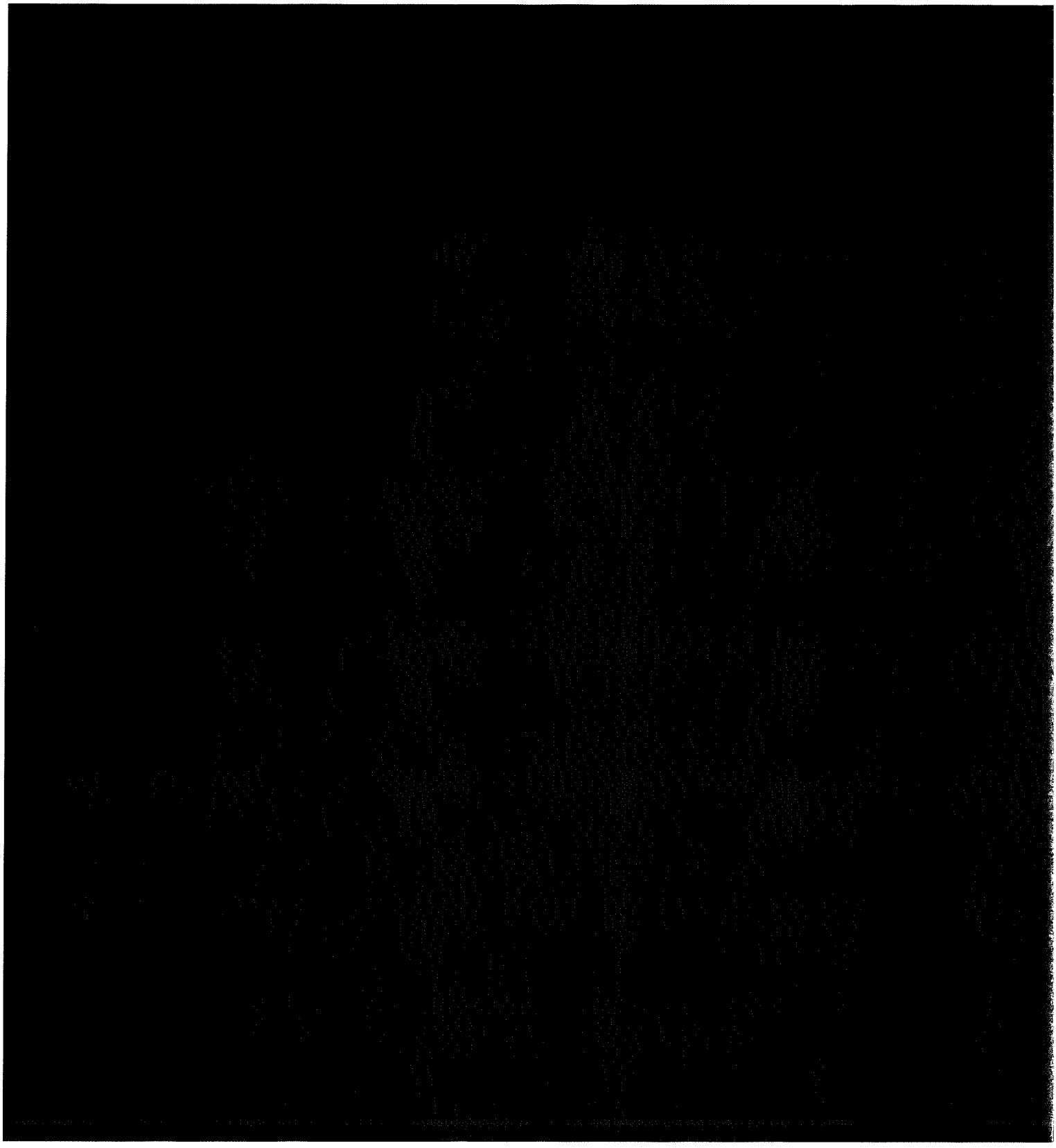


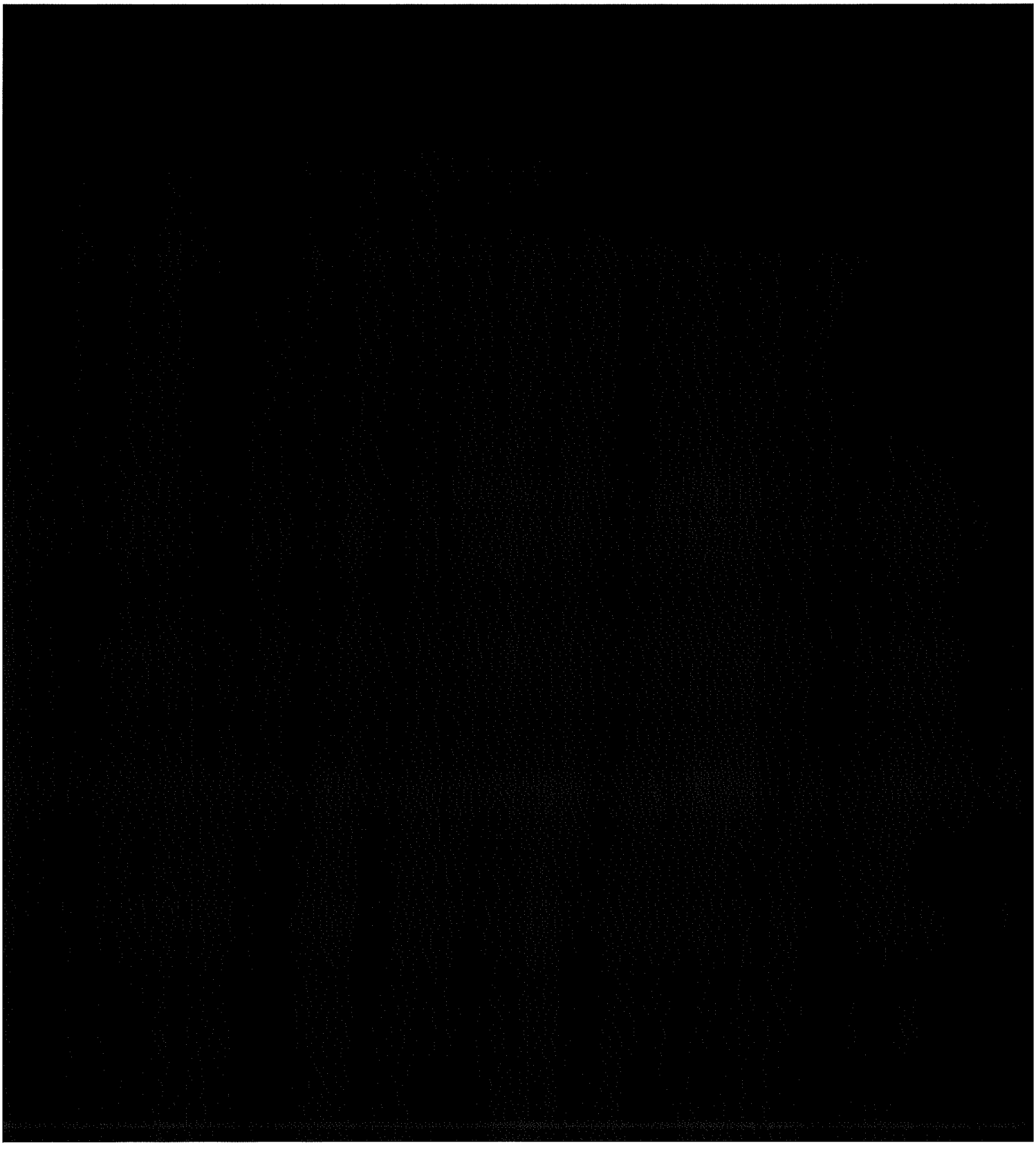












4 Document Scanners and Reader Instruments

Document authentication instruments are devices which provide the DAAT tool with all necessary data to carry out the border crossing procedure, regarding the validity and credentials of required documents (passports, visas, id cards, etc.). The document authentication instruments must provide the Portable Unit (PU) system with the information about any signs of falsification or counterfeiting the travellers' documents.

Additionally, if the traveller has the QR code provided by the iBorderCtrl system (in the pre-registration phase), the document authentication instruments will be able to scan it and provide the system with all information previously uploaded by the analysed person.

To let the traveller into the EU, the following conditions must be fulfilled:

- The presented documents must be considered genuine
- The traveller, based on the information extracted from documents, must be considered harmless
- The traveller has to be entitled to enter the EU (for example, based on the valid visa)

The following review identifies the necessary document authentication instruments that will be used to capture all necessary input. The focus is on the following devices:

- RFID chip readers, required to acquire biometric data stored in passports
- QR code readers, used to acquire the QR code generated during the preregistration phase
- document scanners, used to read documents provided by the traveller: passports, visas, etc.

The detailed description covers technical parameters of these devices such as the interface type, the ability to work in harsh conditions, or mechanical specifications either commercially available or in the research stage. As the result, the selection of the optimal devices from the point of view of the PU system functionality will be proposed. They all should meet functional and technical requirements of the system.

The review describes advantages and disadvantages of the presented devices and indicates the best modules to be used in the final version of the project.

4.1 Document Scanners

4.1.1 Background knowledge

Referring to ICAO 9303 Part 2, in order to verify traditional or innovative security features of the MRTDs the readers should be equipped with the appropriate hardware sensors. For the purpose of the MRZ reading and image processing we need to be able to acquire the document image in the visible (VIS), ultraviolet (UV) and infrared (IR) ranges with high resolution (minimum 300dpi). Moreover, we need to be equipped with the IC readers compliant with ISO 14443 13.56 MHz. Typical readers usually are able to provide the following features:

- MRZ read and check digit verification

- Contactless IC read and Passive Authentication (and, optionally, Active Authentication)
- Generic security checks (UV dull paper, IR readable MRZ, etc.)

There are also features depending on the software providing the processing functionality of data acquired from hardware sensors:

- Pattern recognition using databases (based on VIS, UV and IR images)
- Reading and authentication of digital watermarks (steganographic features) for authenticity checking
- Detection and reading (alphanumeric) for displaying and their future security features
- Detect and read out LED-in-plastic based security features

Advanced document readers may be equipped with hardware sensors that allow users to exploit special security features:

- Coaxial illumination for the verification of retro-reflective security overlays
- Laser diode or LED illumination for the verification of special structure features, e.g. for optically diffractive devices (DOVIDs)
- Magnetic sensors for special substrate features, e.g. for the verification of magnetic fibres;
- Spectral analysis or polarization detection devices
- Illumination of the MRP data page for the verification of registered watermarks, laser perforation, window features and see-though registers –a special reader geometry to allow for the placement of the data page only on the reader is required

Advanced reading capabilities are all based on national/bilateral agreements and require dedicated hardware.

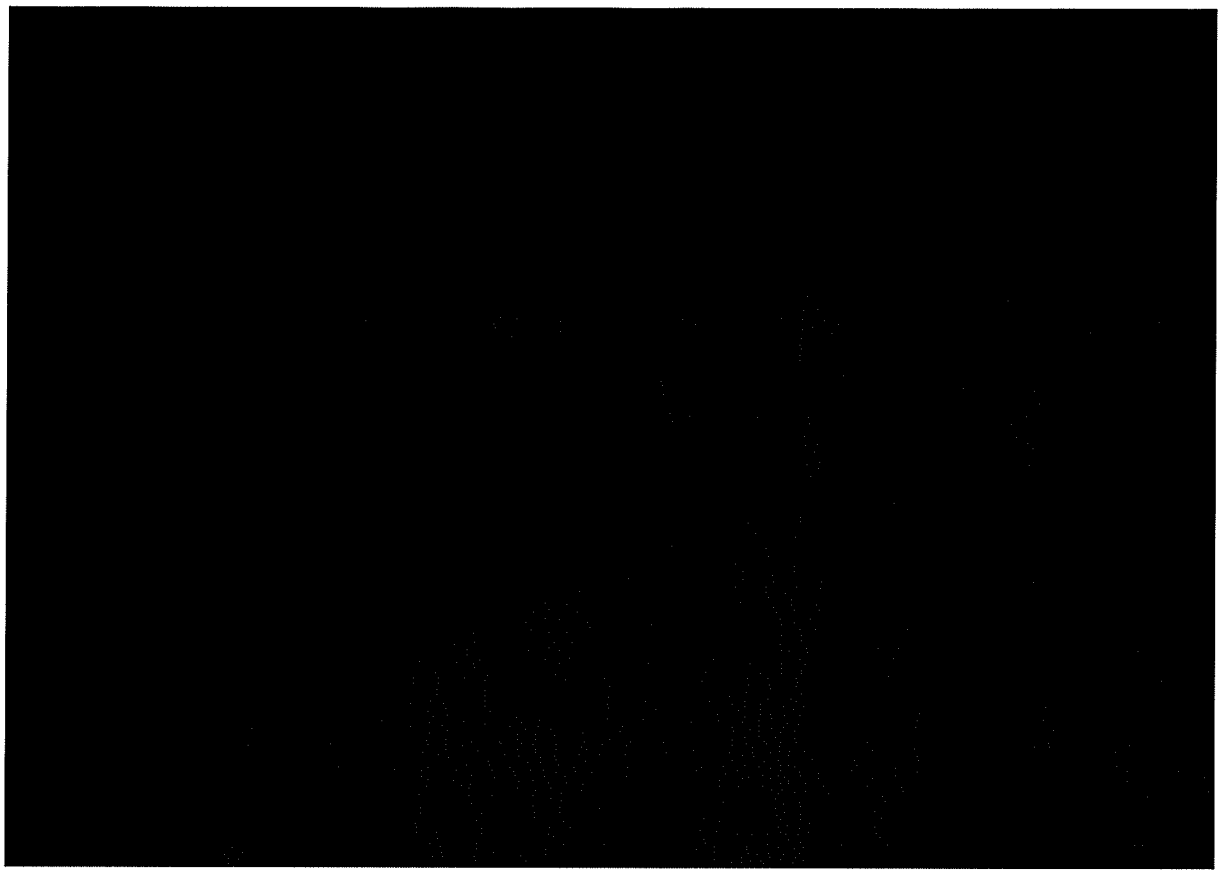
To arrange authenticated connection between IC and RFID reader, PKI (Public Key Infrastructure) may be required. It is used to authenticate data stored in the RFID passport chip, making counterfeiting it difficult and expensive.

Based on the document "The fourth generation of ePassport" by Gemalto in June 2014, the first generation ePassports was based on Basic Access Control (BAC). This data access mode introduced to prevent skimming, eavesdropping and securing data stored in ePassport IC (biographic and facial image). BAC is a symmetric protocol and the authentication relies on the data provided in the MRZ on the data page. Before the device is granted the data access, the chip and reader mutually authenticate themselves using a specific authentication key derived from the MRZ (also used to generate session keys for the encrypted data exchange).

More secure and reliable is EAC (Extended Access Control) mode used in the second generation of ePassports (more biometric data – fingerprints or iris pattern – added to IC:) has been introduced. To get access to the data, the reader has to present valid chain of certificates. Its root contains the public key associated with:

- Document Verifier certificate of the welcoming country signed by the issuing country
- Inspection System certificate signed by the welcoming country

If 'Country-A' wants to allow 'Country-B' to access its citizens fingerprints, the former has to sign DV keys of 'Country-B'.



4.1.2 Sensors and devices

Mobile Document reader Regula 7308.100/110/111[11]

This is the mobile compact size model with a shoulder strap. Its body is made of hard plastic (compliant with the IP54 norm). The hardware capabilities (with a built-in PC) allow for the full data acquisition and processing. The reader is connected to the external PC or any other visualization device (tablet, smart phone, etc.) via the wireless network (Wi-Fi). Power supply includes two rechargeable batteries (with the hot swap capability). There are no moving parts, decreasing the threat of physical damage. The device captures images in coaxial light, VIS, IR and UV light. It has a module for reading RFID information. Optionally, it can be equipped with a module for reading smart cards. The device is supplied with software development kit (SDK) for easy integration into existing end-user systems.

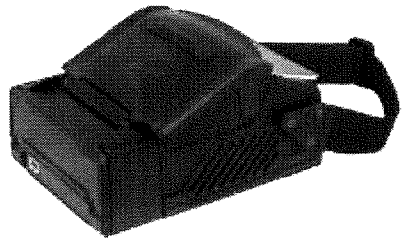


Figure 5 Mobile Document reader Regula 7308.100/110/111

[11] https://regulaforensics.com/en/products/machine_verification/7308/

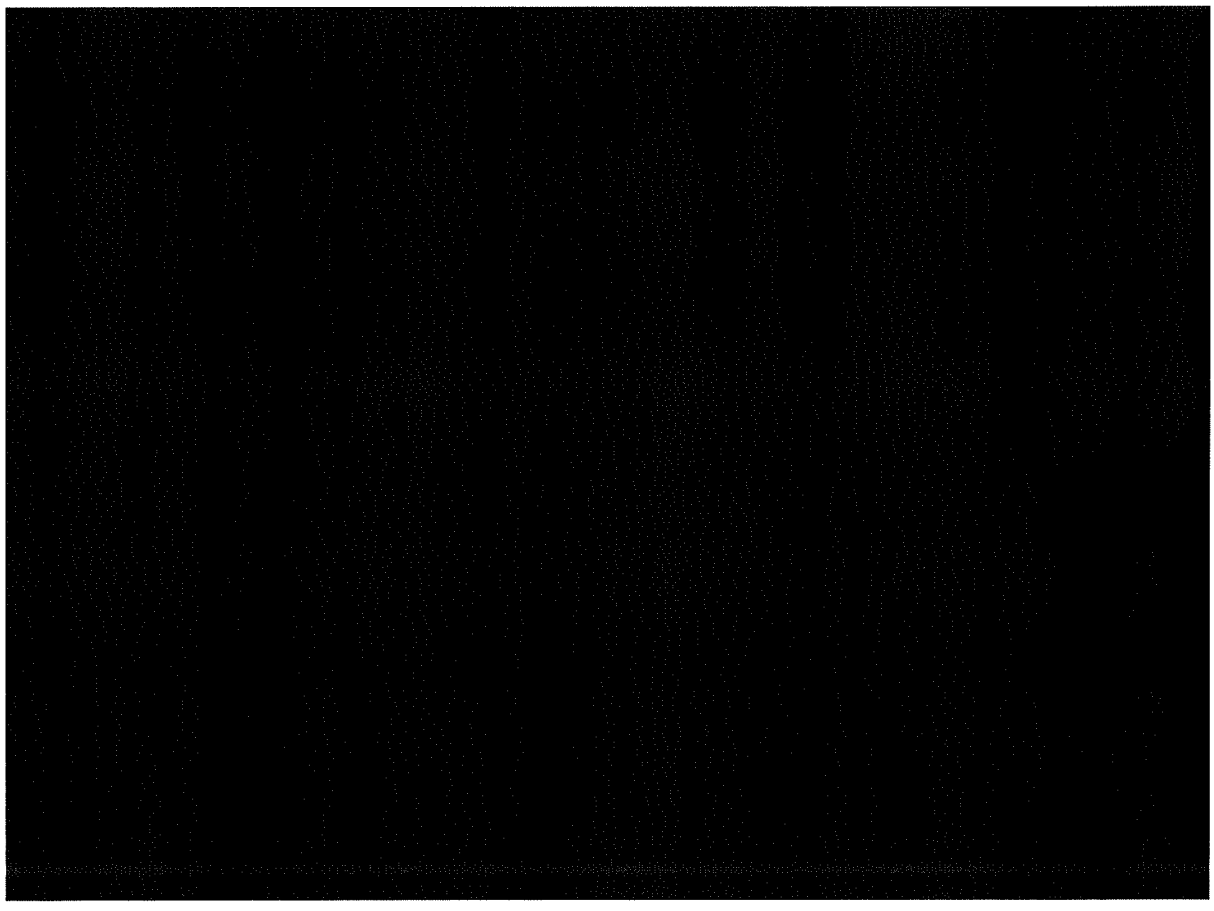
Its key features include:

- Mobile document scanner with three light sources
- Full passport scanning
- Not less than 7.5 hours operating time
- Regula software SDK
- Microsoft OS compatibility
- Optical Character Reading (OCR) support
- Scanning the bio-data page of document (embedded RFID microchip ISO 14443, type A and B) at the border control check
- Reading the Machine Readable Zone (MRZ) of the travel document
- 24-bit colour depth, RGB, CMOS sensor
- 1D and 2D barcodes reading
- Document recognition type
- Analysis and comparison of text data
- Automatic authenticity verification
- Recognition and reading 1D and 2D barcodes

Supported formats:

1D: Code, Code39 (+extended), Code93, Code193, EAN-8, EAN-13, IATA 2 or 5 (Airline), Interleaved 2 of 5 (ITF), Matrix 2 of 5, STF (Industrial), UPC-A, UPC-E

2D: PDF417, Aztec Code, QR Code, Datamatrix



FS531-U passport and card scanner[12]

The ScanShell 1000N passport scanner is prepared for high resolution scanning and driver license. It is characterized by user friendly interface, compact size and weight with flat design. The scanning result is the document image in VIS and IR spectra.

Key features:

- Flatbed passport scanner
- Light source: visual, infrared spectrum
- 3 to 12 seconds per scan
- No external power needed - USB connection
- Twain compatible
- Auto-detect function
- Fully portable small print passport scanner
- 24bit colour depth, RGB, CMOS sensor

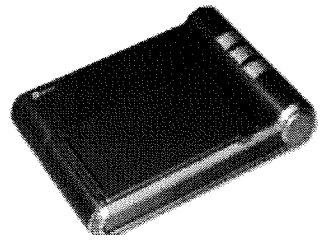
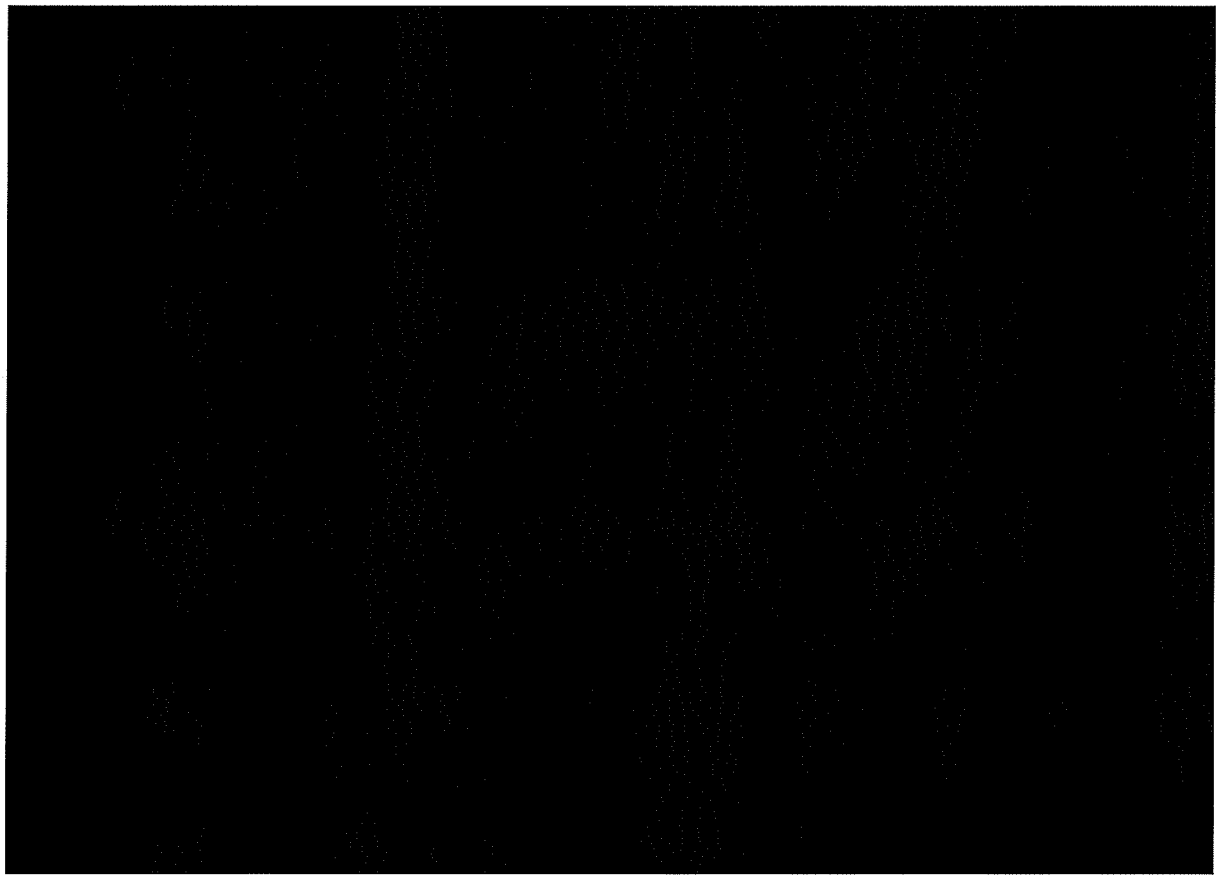


Figure 6 FS531-U passport and card scanner



[12] http://scansys.com.sg/IDScanner.aspx

Vicomp 460 optical passport reader

The VPR-460 passport reader[13] is a specialized device for reading the OCR-B information from machine readable passports, which comply with the regulations of ICAO and ISO 7501 standards. The reader is operated with a single hand-swipe motion (left-to-right or right-to-left), and captures two or three machine-readable codelines simultaneously. Bluetooth link is used for reader–host communication. The VPR-460e variant uses the built-in RFID reader to retrieve data from e-passports.

Figure 7 Vicomp 460 optical passport reader

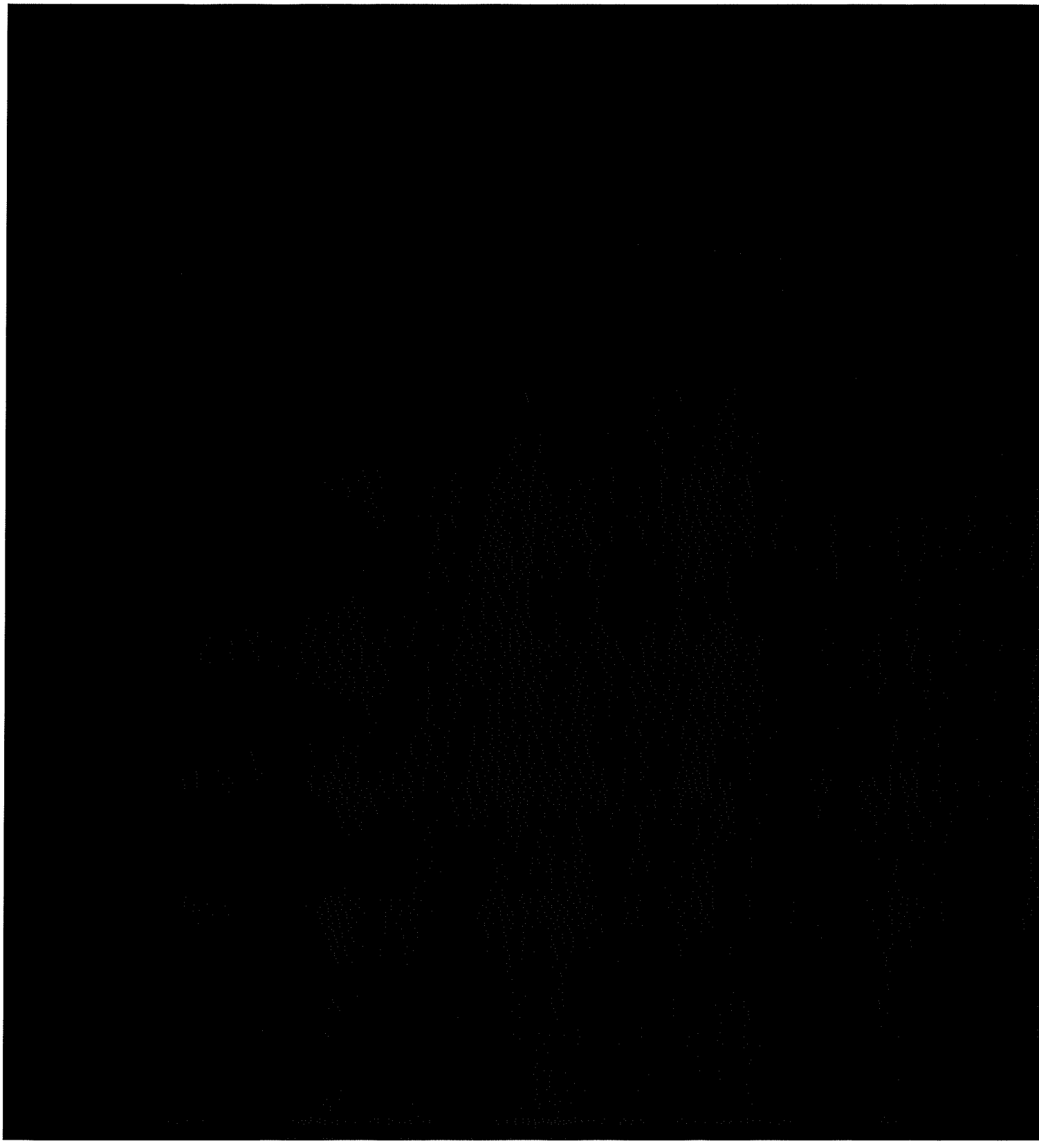
The reader is powered by an internal battery pack (2xAA), which assures up to 4000 documents readings (OCR + RFID). When not used, it enters the "sleep mode".

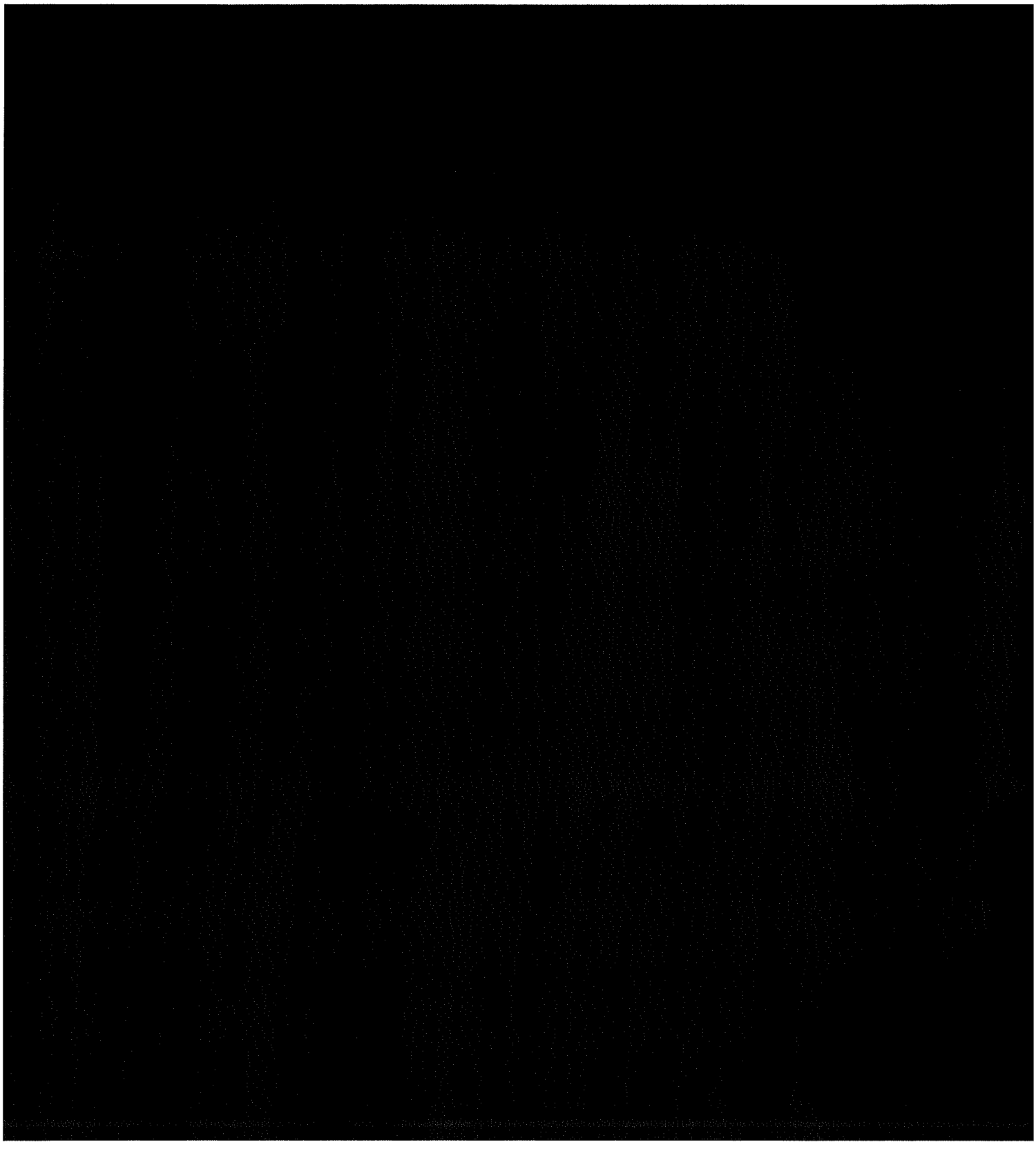
Key features:

- Hand swipe operation
- No moving parts
- Power saving (auto power on & off)
- Efficient reading algorithm
- Minimal operator training
- Compact style
- Low error rate
- Wireless interface

[redacted]

[13] https://vicompnew.jimdo.com/hardware/





[redacted]

4.2 RFID chip readers

4.2.1 Background knowledge

Radio-frequency identification (RFID) uses electromagnetic fields to identify and track tags attached to various objects. Passive tags collect energy from nearby RFID reader-originated radio waves. RFID tags are used successfully in multiple applications allowing for electronic storage of information in small, cheap and passive components. Technical details of RFID (coding type, tag memory size, baud rate, etc.) are described in many standards. Two main standards for RFID technologies exploit frequency of 13.56 MHz. The ISO 15693 standard offers longer read ranges, but slower data transfer (26K baud). Another one, ISO 14443 offers shorter read ranges and faster data transfer (106K baud). Biometric passports are equipped with chips implementing ISO 14443 standard.

[redacted]

4.2.3 Sensors and devices

SmartScanndy 2 HF

SmartSCANNDY[14] was designed for capturing data and Real Time (RT) transactions. It weighs 80g and is the lightest hybrid AutoID device in its class, fitting into the pocket. It is resistant to dust and water, surviving downfalls from a height of 1.5 m on the concrete floor.

[14] http://www.agillox.com/en/products/all-products/product.php?we_objectID=159&c=8

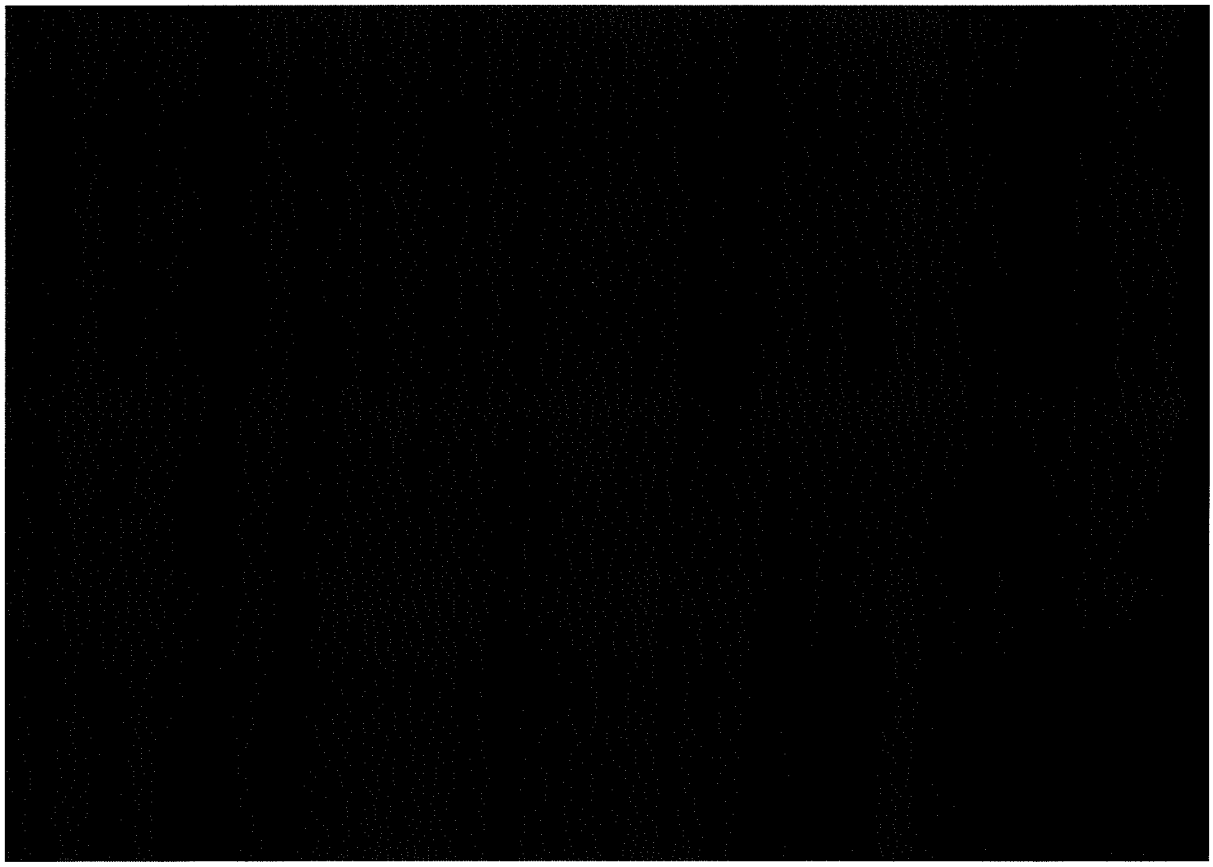
PanMobil smartSCANNDY is controlled by the embedded Linux OS. Its functions include the 1D/2D barcode reader and/or RFID reader/writer for various RFID frequencies and standards. It comes with the 233 MHz ARM processor.

Figure 8 SmartScanndy 2 HF Reader

Data acquisition is performed by the following modules: barcode scanner, 1D Laser, 1D Imager,1D and 2D Imager, RFID reader/writer for low (125KHz band), high frequencies (13,56MHz band compliant to the ISO15693 norm and 13,56MHz band compliant to the ISO14443A norm) and ultrahigh frequency Mifare standard (868-940MHz band) with EPC Gen2 communication standard. Optional modules include Bluetooth (with SPP and HiD profile), USB interface with Quad USB functionality (USB memory stick, USB HiD, USB serial, USB Ethernet).

Key features:

- Functionality: barcode scanner for 1D and 2D codes, RFID reader
- Communication standards: Bluetooth, USB and Wi-Fi
- Operating system: Embedded Linux
- Vibration (optional)
- Programming interfaces for C/C++
- Durability standards: IP54 rated, 1.5 meter fall threshold



Gao RFID 13.56 MHz Handheld Bluetooth RFID Reader

The 13.56 MHz handheld Bluetooth RFID reader[15] incorporates both USB and Bluetooth data transfer options and is NFC compatible. It is compact (size of the human palm) and widely used in such applications as access control, item/people tracking or security.

Figure 9 Gao RFID 13.56 MHz Handheld Bluetooth RFID Reader

Gao RFID 13.56 MHz Paddle Reader w/Bluetooth

This 13.56MHz RFID reader[16] has both read and write capabilities for compatible tags. It is easily integrated with a wide variety of mobile computers via Bluetooth. The GPS module facilitates tracking the geographical position of the scanned object.

Figure 10 Gao RFID 13.56 MHz Paddle Reader

Key features:

- Handheld, ergonomic styling
- Lightweight, small size
- Powered by rechargeable Lithium-Ion battery
- Available with ActiveX controls for Microsoft Windows application programmers undertaking software integration
- Equipped with Bluetooth GPC location devices for asset mapping

[15] http://gaorfid.com/product/reader-bluetooth-paddle-hf-13-56-mhz-rfid/
[16] http://gaorfid.com/product/reader-handheld-bluetooth-hf-13-56-mhz-rfid/

Jett RFID+[17]

This device has the Marvell XScale Technology processor and runs on Microsoft Window CE 5.0 operating system. The RFID module operates on the HF 13.56MHz frequency, supporting ISO 14443A, ISO 14443B and ISO 15693 standards, implemented in tags from major manufacturers.

The mobile computer reads tag IDs, reads and writes data blocks, authenticates and encrypts data to and from compatible tags. These capabilities support secure storage of private information, required in such applications as healthcare, access control and mobile commerce. The antenna allows for reading tags at any angle.

The device is highly customizable, regarding the case colour, protective bumpers, keypad, logo tag, serial tag, or additional cables. The disadvantage is the relatively large size and heavy weight. Advantages include flexibility and customizability.

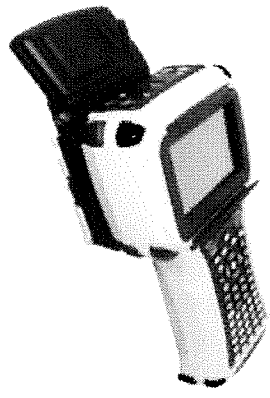
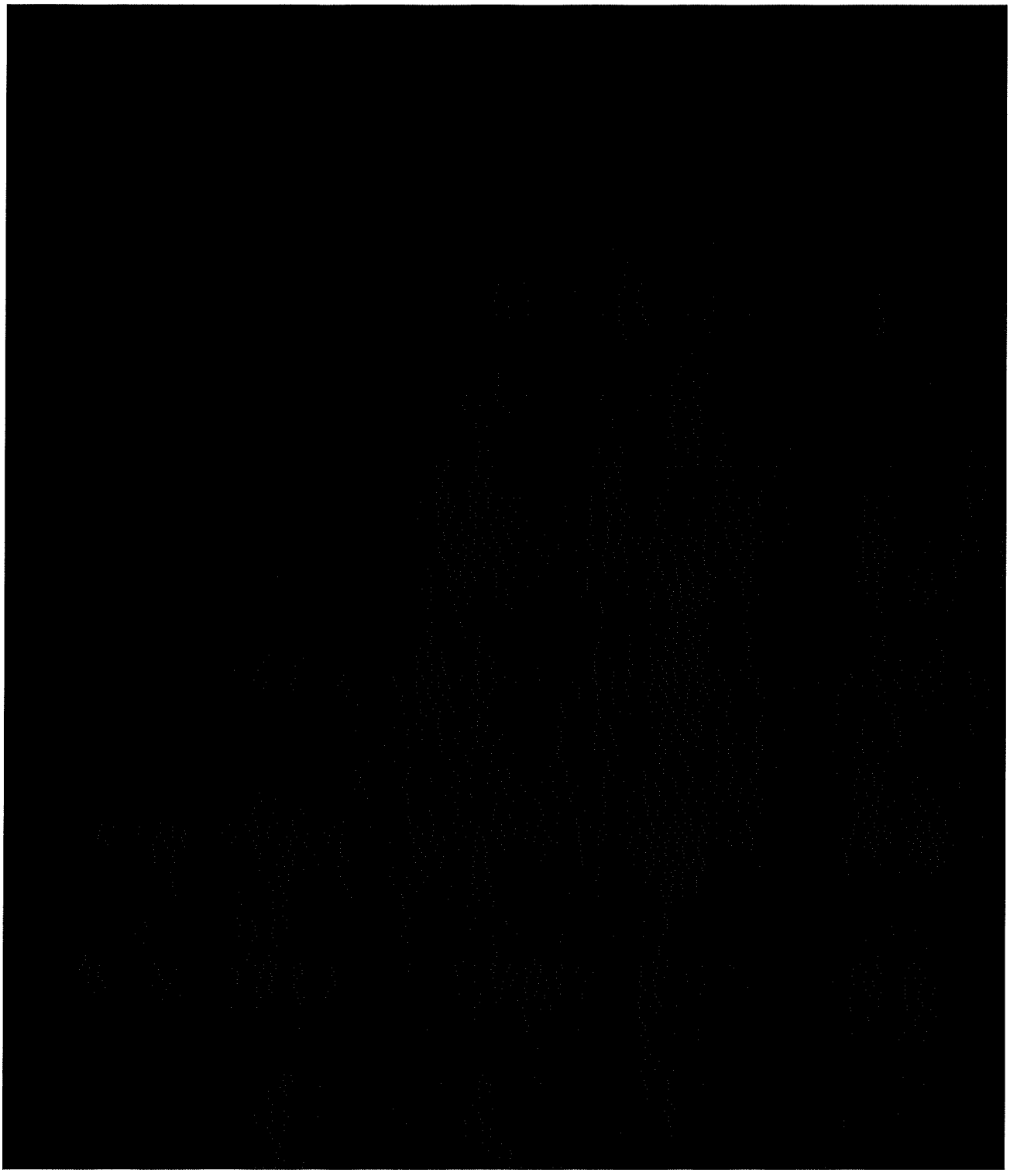


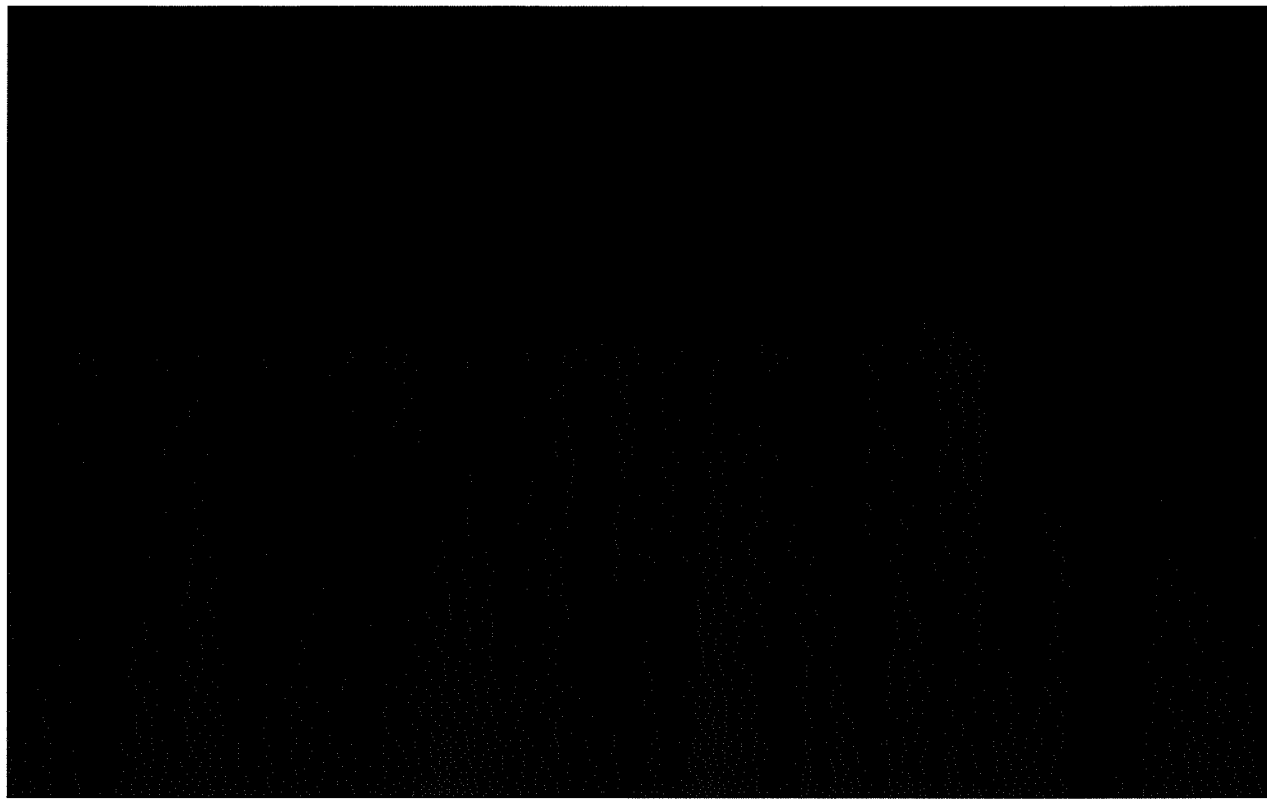
Figure 11 Jett RFID+

Key features:

- 13.56 MHz EFID Enabled
- IP65 ingress protection
- Microsoft Windows CE 5.0
- Marvell Xcale PXA270 technology processor 624 MHz
- 320x240 QVGA-TFT colour sunlight readable display with touch screen
- 9 hours typical operating time (actual time may vary based on a variety of conditions)
- CF Type 2 accessible expansion slot
- Standard Stylus

[17] http://www.2t.com/jett_rfid.asp





4.3 QR code scanners

4.3.1 Background knowledge

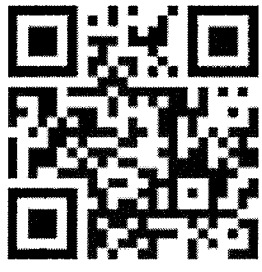


Figure 12 QR Code Image

In contrast to one dimensional barcodes designed to be mechanically scanned using the narrow beam of light, the QR code is read by a 2-dimensional digital image sensor e.g. VIS camera and then digitally analysed by the programmed processor. It locates three distinctive squares at the corners of the QR code image, using the smaller square (or multiple squares) near the fourth corner to normalize the image for size, orientation and viewing angle. Small dots throughout the QR code are then converted to binary numbers and validated by an error-correcting algorithm.

Commercial laser scanners cannot read complex 2D symbologies[18] such as QR code or Datamatrix. Due to the nature of the light, only single thin (linear) slice of the barcode can be read at a time. There is no sweep pattern of the laser that can survey the entire 2-dimensional barcode. To achieve this, the 2D imager is required. Laser scanners can read linear barcode symbols such as Code 39, Code 128, UPC and others. Some lasers read 2D-like symbolic patterns called PDF-417, commonly used for postage and some inventory

[18] The mapping between messages and barcodes is called a symbology. The specification of a symbology includes the encoding of the single digits/characters of the message, as well as the start and stop markers into bars and space; the size of the "quiet zone" before and after the barcode; and the computation of a checksum. The spaces and bars of a barcode are a simplified language (COBOL, BASIC and FORTRAN) that allow programmers to speak with computers.

applications. Additionally, lasers may not scan barcodes on screens as they do not reflect the laser light properly.

In the CCD (Charge Coupled Device) linear imager, LED is used to illuminate the barcode. Tiny CCD sensors are aligned in a single row to read and decode the light reflected from linear barcodes. The device operates as a camera taking pictures in the form of single row of pixels. Being linear, these devices are unable to read 2D barcodes.

Algorithm performance

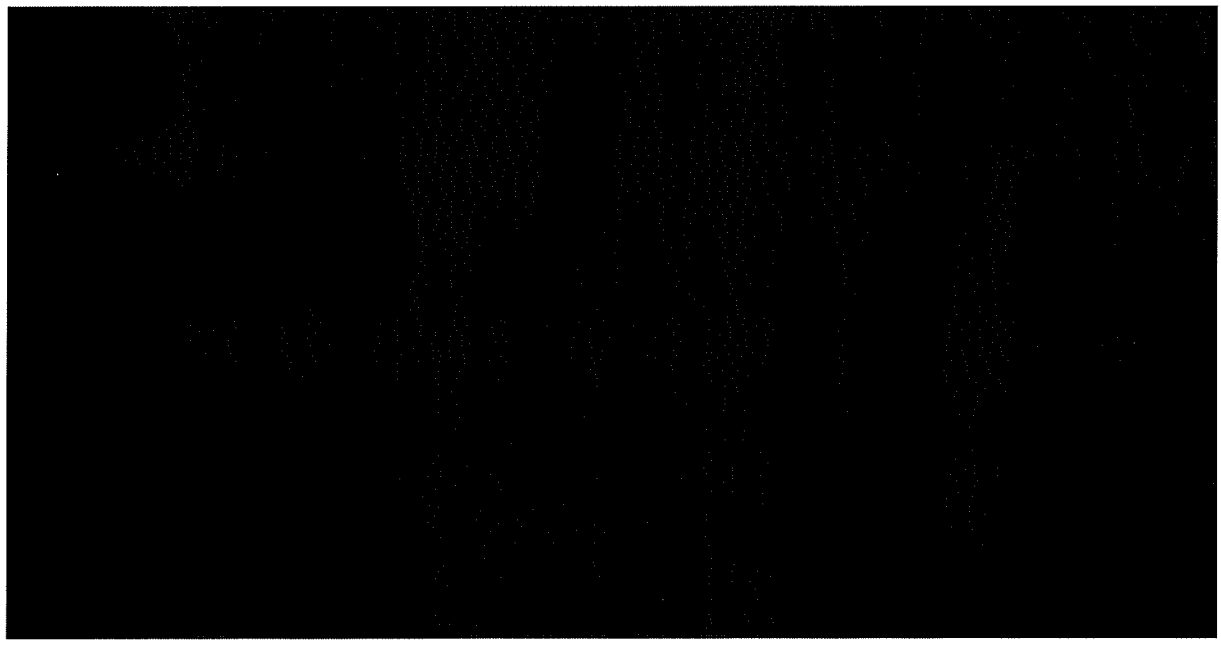
The imager works by taking pictures and running image processing algorithms on each image to detect barcodes. The algorithms seek to find whichever barcode symbology the device has been configured to focus on. The fewer the patterns the device looks for, the faster it can be. The scanner performance can be drastically improved just by turning off symbologies that aren't needed.

Barcode scanning also depends on the speed of the CPU and GPU (Central Processing Unit and Graphics Processing Unit, respectively). The latter is optimized for graphics and image processing. Images taken by the camera need to be processed as quickly as possible. This requires fast and efficient CPU.

QR code standards

Symbols described by the QR Codes range from Version 1 to 40. The choice of the version depends on the amount of data to save. For example, Version 3 with Level M (medium) error correction rate consists of 101-digit numerals. Each of them has a different module configuration or the number of modules (where module refers to the black and white dots that make up the QR code). The module configuration refers to the number of modules contained in a symbol, starting from Version 1 (21 x 21 modules) up to Version 40 (177 x 177 modules). The next version number introduces 4 additional modules per side compared to the previous one.

Each QR code symbol version has the maximum data capacity according to the amount of data, character type and error correction level. As the amount of data increases, more modules are required to comprise the code, resulting in larger symbols.



4.3.3 Sensors and devices

Code Reader 2600 Scanner[19]

This is compact and lightweight device, available as palm- and handheld. Disadvantages include speed or code reading and processing in all directions and wide variety of angles. Charging stations allow for recharging the battery within 4 hours (via USB) or 2-3 if the AC power supply is used. Communication between the device and the host is provided by Bluetooth.

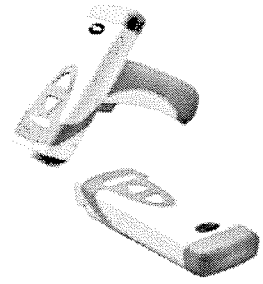


Figure 13 Code Reader 2600 Scanner

Key features:

- Durable, quick-release rechargeable battery cartridges
- Battery status LED indicators with fuel gauge
- User feedback with vibration, audible tones and LED
- Dual field optics, both high density and wide field in the same unit
- Glare reduction technology for reading barcodes on shiny surfaces
- Omnidirectional reading of 1D, 2D and Postal barcodes
- Multiple programmable buttons for customized work flow processes
- Bluetooth support for Android, iOS, and Windows mobile devices and tablets
- Easy to clean, disinfectant-ready CodeShield™ plastics and IP65 housing
- Paging button to assist in locating reader (Charger Station with embedded CodeXML® modem option only)
- Ability to read barcodes from cell phone screens
- CortexRM® Remote Management ready
- Data processing abilities using JavaScript

[redacted]

[19] http://www.codecorp.com/products.php?id=138

[redacted]

RS6000 1D/2D Bluetooth Ring Scanner[20]

This is the durable scanning, finger-worn device with long endurance battery. Communication with the host is obtained via Bluetooth communication technology. The 650nm laser is used for targeting the code. The optical resolution is 1280x960 pixels.

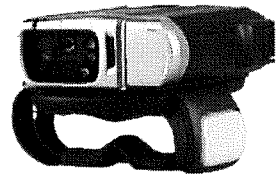


Figure 14 RS6000 1D/2D Bluetooth Ring Scanner

Key features:

- Fast capture of barcodes
- Hands-free scanning
- Ambidextrous trigger button and mounts
- Tap to pair to create a Zebra total wearable solution in seconds
- No Wi-Fi interference guaranteed
- Bluetooth power efficiency
- Flexible manual or automatic triggering
- New comfortable and hygienic mount

[redacted]

[20] https://www.zebra.com/us/en/support-downloads/mobile-computers/wearable-computers/rs6000.html

[redacted]

RS507 Hands-Free Imager[21]

This ergonomic and rugged device is mounted on two fingers, able to communicate with the host via Bluetooth, although corded version is also available.

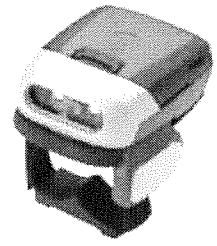


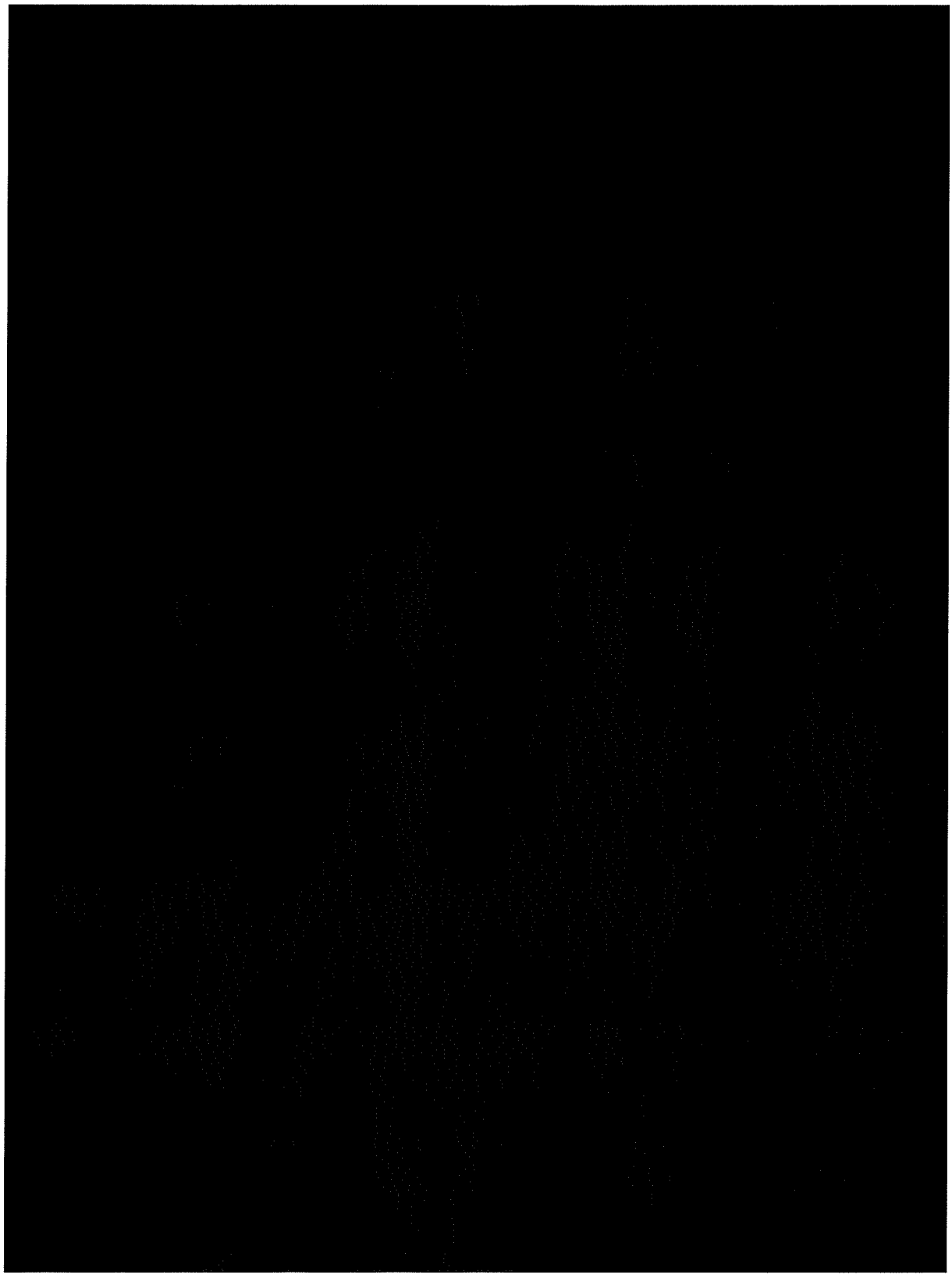
Figure 15 RS507 Hands-Free Imager

Key features:

- Hands-free scanning
- Exceptional motion tolerance
- Aiming pattern by the laser dot (650nm)
- Rugged class
- Enterprise Mobility Developer's Kit
- Battery age testing
- RoHS compliant

[redacted]

[21] https://www.zebra.com/us/en/support-downloads/mobile-computers/wearable-computers/rs507.html



5 Tablets

5.1 Background knowledge

The tablet computer, shortened to tablet is a portable PC, usually with large LCD touchscreen and mobile operating system. Tablets are equipped with rechargeable battery and their functionality is the same as for standard PCs, with extended functionality known from smartphones. These devices, due to their size and performance, found their place in multiple aspects of live. Tablets typically have I/O capabilities that suit them to their usual tasks. These may include front and rear cameras, fingerprint sensor, GPS, barometer, flashlight, gyroscope, microphone, Bluetooth and Wi-Fi receivers. Variety of models allow for selecting larger or smaller computer, more or less powerful. Tablet market has grown fast because of reasonable prices of devices, omnipresent Wi-Fi network in public places and social media. Availability of portable PCs revolutionized many branches of technology allowing them to implement brand new solutions for huge amount of projects and ideas, reducing costs, space and weight. Computing power of tablets is still increasing, making them suitable for solving complex computational problems. Devices dedicated to work with large amounts of data easily fulfill their tasks.

5.2 Reference to the architecture and technical requirements

The main tablet functionality is to send data from DAQ devices connected via Wi-Fi/Bluetooth/USB to the iBorderCtrl servers. It must be equipped with the software necessary to meet project goals. Some of the captured data (i.e. from document scanner and body mounted camera) should be visualised on screen allowing an officer to easily interpret results and take necessary actions. The tablet being the part of the PU must be light. Secondly, it has to work for a long time on the battery. This feature is the most significant, as PU will be used in the completely mobile environment. The next important requirement is durability. Computers will be operating in the external conditions (roads, forests, etc.), so they have to be resistant to harsh conditions, such as wide range of temperature change, high humidity and shock. The computing power of the device is also important. Operations performed on-site (such as the fingerprint verification) should be optimized.

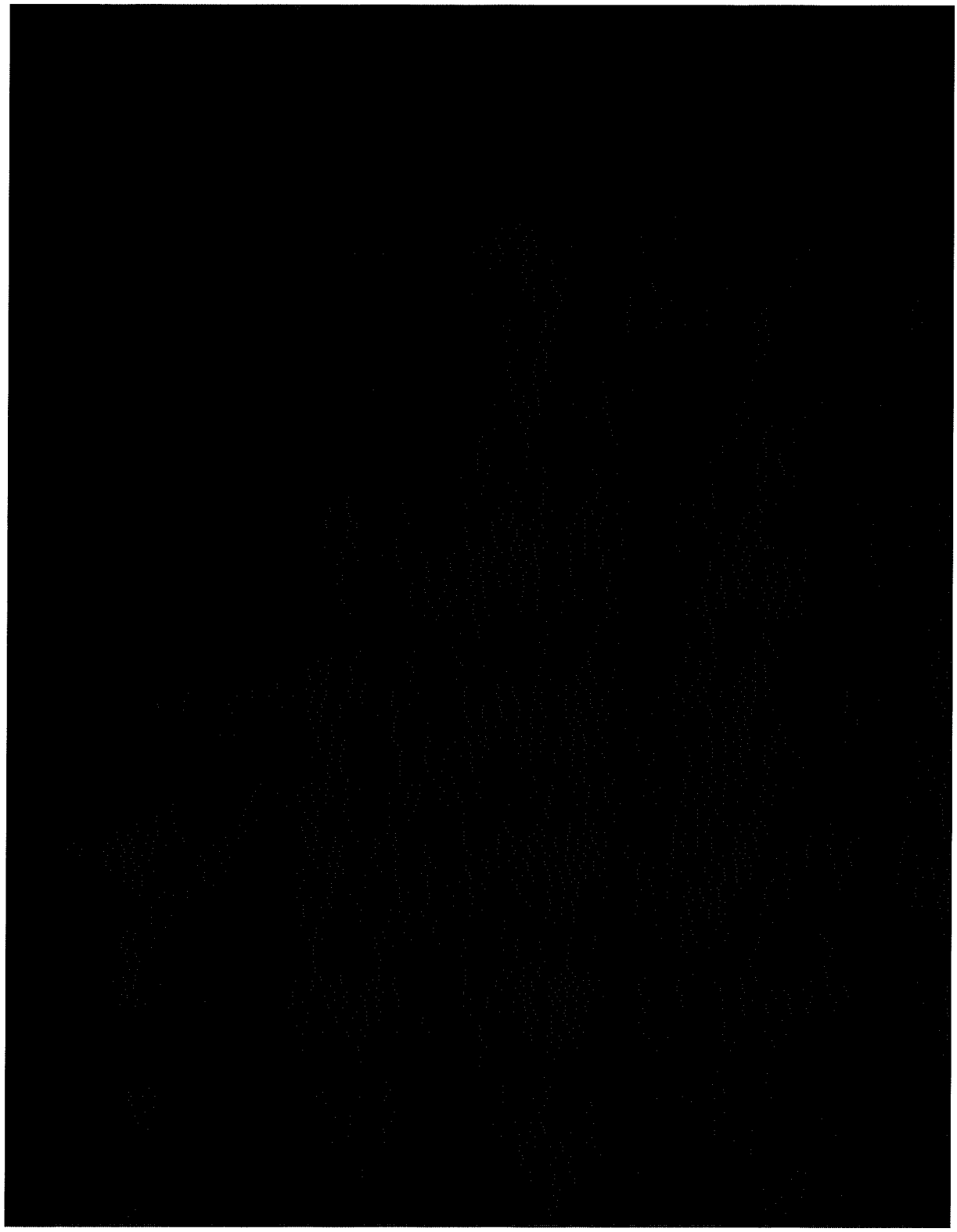
5.3 Devices

5.3.1 Getac T800[22]

Figure 16 Getac T800 Tablet

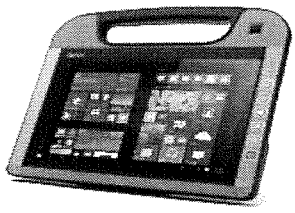
T800 is a lightweight (0.88kg) and durable tablet, tightly packed and with robust design. The 8-inch LumiBond screen with high brightness is big enough to be easily operated in the field. With a specially designed back case, it is possible to connect a smart card reader or RFID reader or an additional HotSwap battery.

[22] http://en.getac.com/tablets/t800/specs.html



[redacted]

5.3.2 Getac RX10[23]

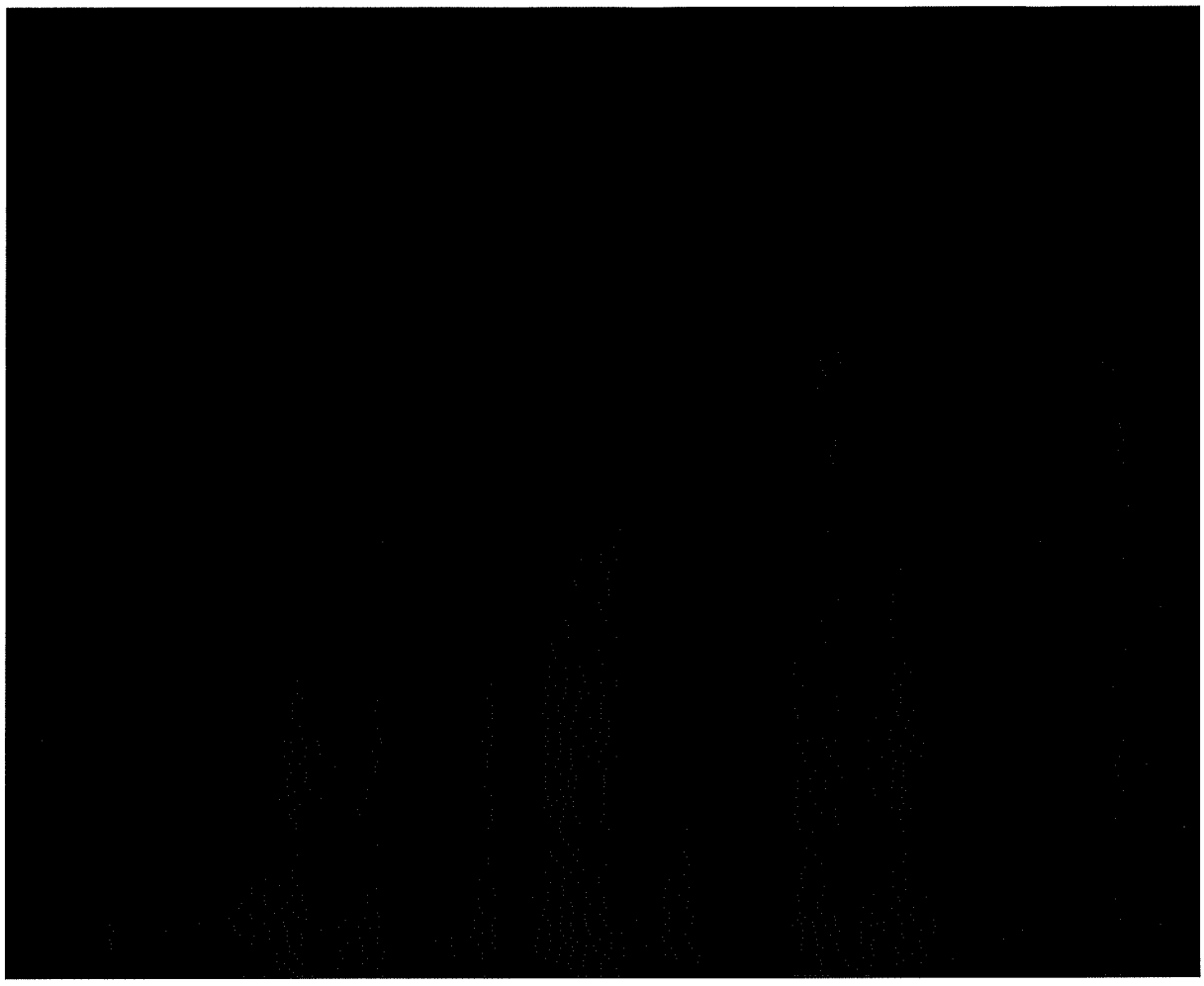


This tablet features the Intel Core M processor. The screen is made with the LumiBond 2.0 technology and the IPS matrix provides the 1920x1200 resolution. The additional feature is the embedded fingerprint reader.

Figure 17 Getac RX10 tablet

[redacted]

[23] http://en.getac.com/tablets/rx10/specs.html



5.3.3 Zebra ET50/ET55[24]

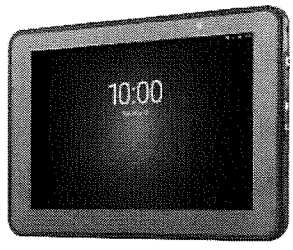
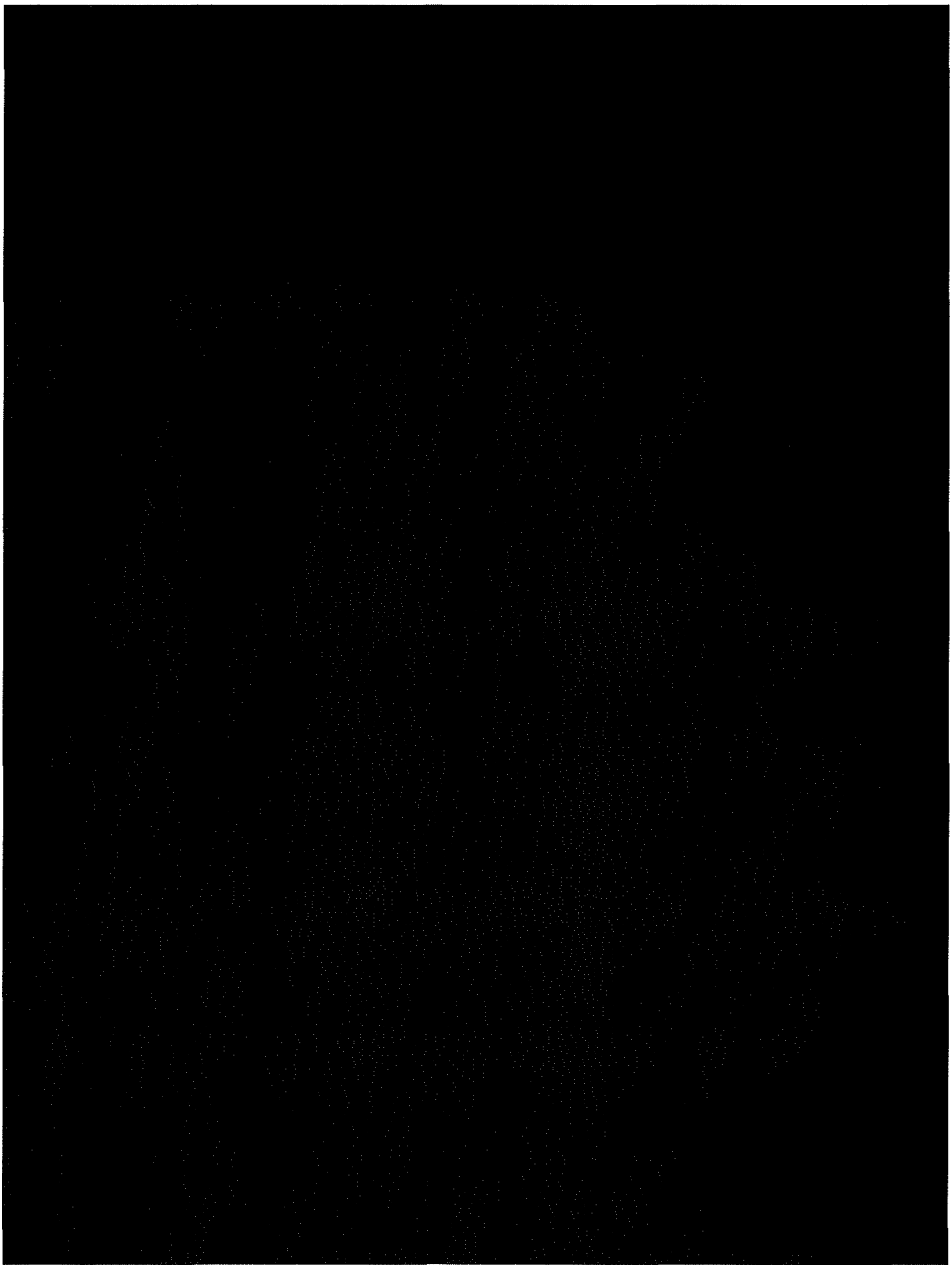


Figure 18 Zebra ET50/ET55

The Zebra ET50 / ET55 is an industry-standard tablet operating on Windows Embedded 8.1 Industry Pro or Android 5.0 Lollipop. The display size is 10.1-inch or 8.3-inch. The wireless communication standards include Wi-Fi, Bluetooth, LTE and NFC. It has the 2.4 GHz Intel Quad-core processor and 4 GB RAM.

[24] https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/product/Tablets/et50-55-enterprise-tablet/spec-sheets/et50-et55-tablet-spec-sheet-en-us.pdf



5.3.4 Fujitsu

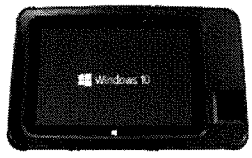
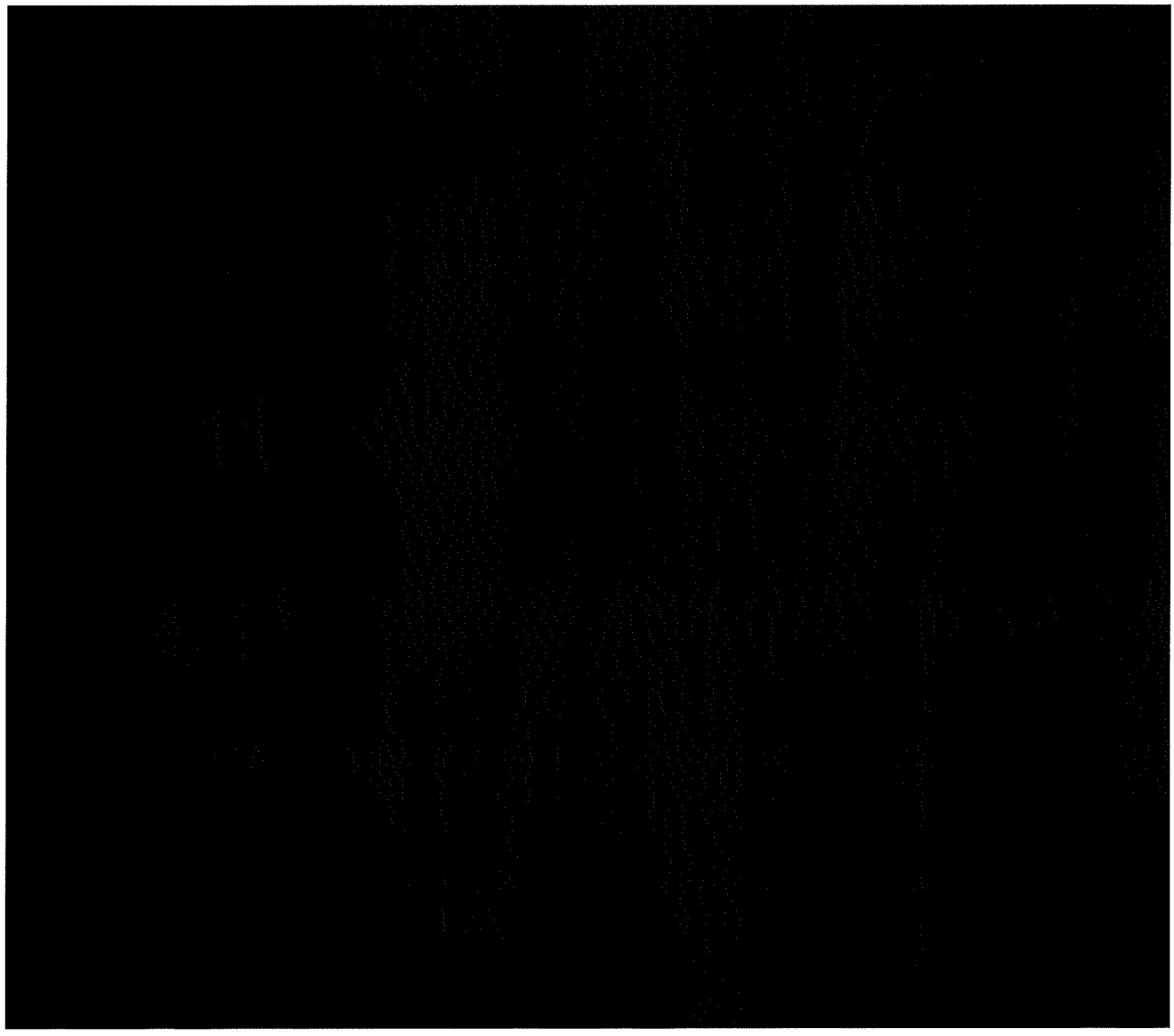
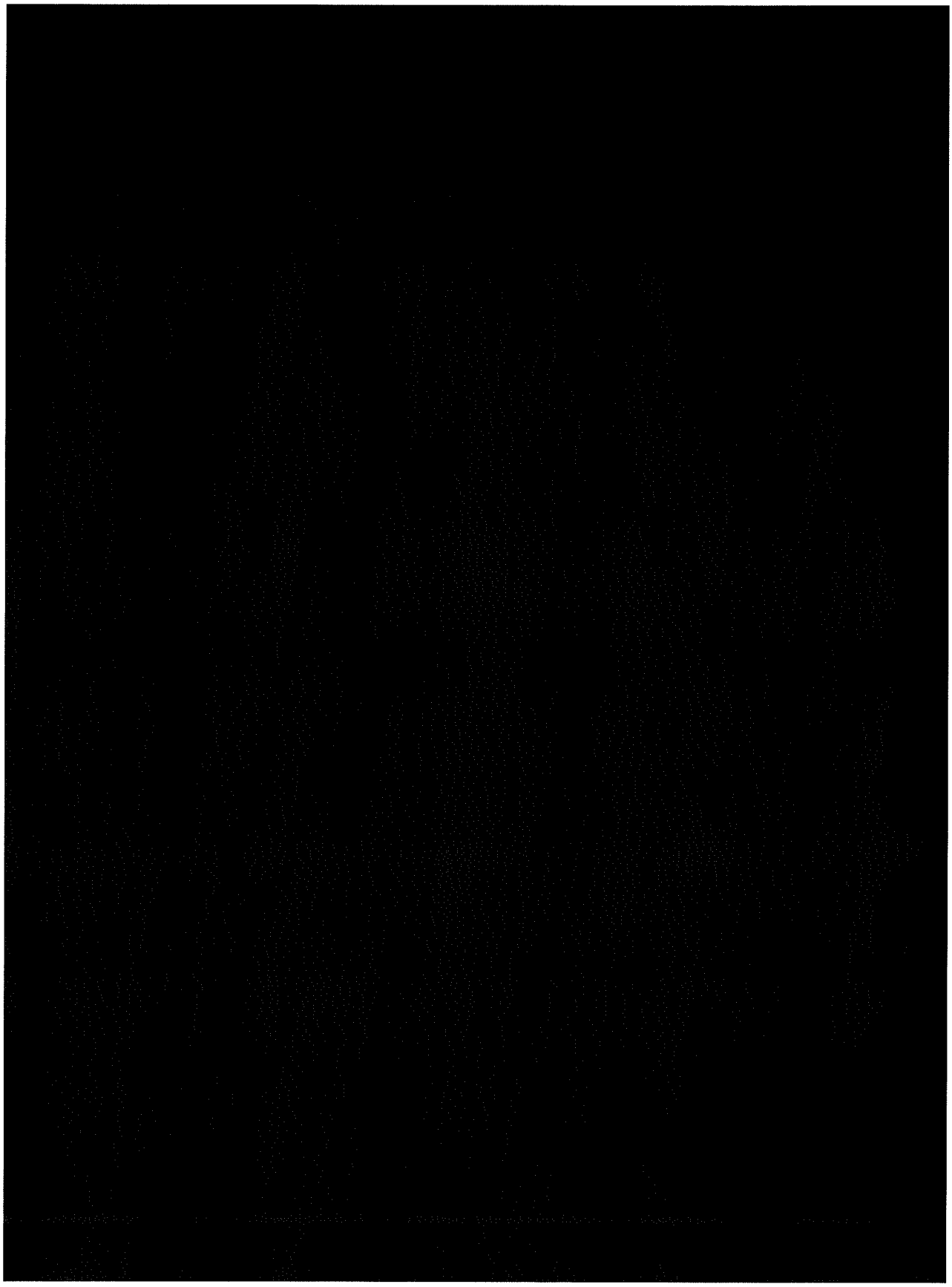


Figure 19 Fujitsu (Biosec) tablet

The FUJITSU/Biosec Tablet is made for rough environments due to water and dust resistant yet lightweight design and combined with a 21.0 cm (8.3-inch) display with toughened glass. Wireless connectivity includes WLAN 802.11a/b/g/n. Equipped with Lithium polymer battery, it allows for working over 5 hours. It can be easily integrated and secured due to Windows 8.1.





6 Detection of Hidden Humans

6.1 Background Knowledge – rationale

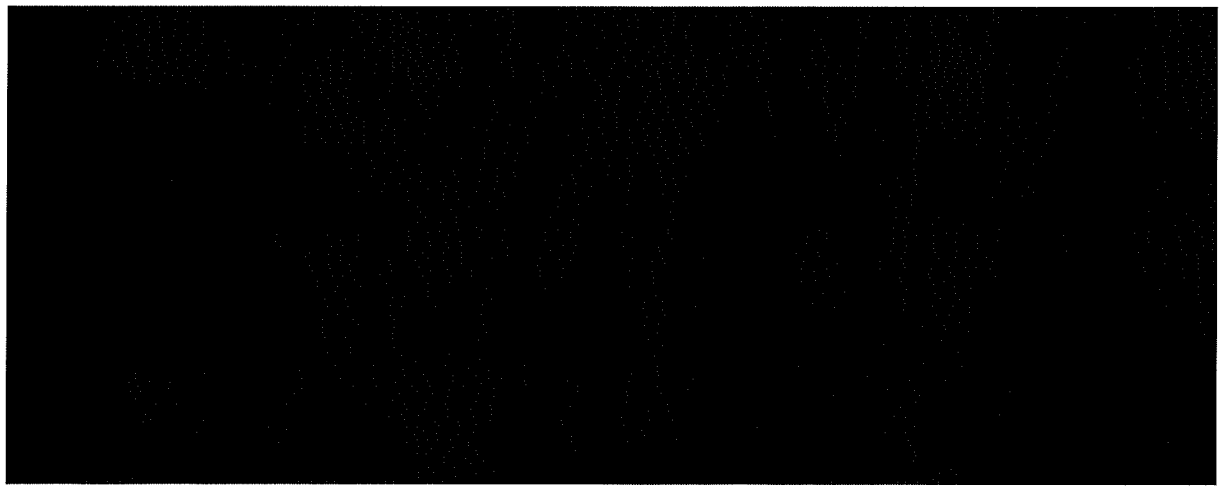
As already pointed out in Chapter 2, currently, the most trending way of illegal border crossing is to cross the green border, second most relevant modus operandi is hiding in vehicles and third but equally important one is impersonation. As it was also analysed in the previous chapters, impersonation and connected spoofing are considered the most important aspect, within iBorderCtrl.

However, the fact that the second most trending way of illegally crossing the borders is hiding inside any kind of vehicles, cannot be neglected or lightly passed over.

Border checking and control of such illegal attempts requires every-day-continuous attention especially in illegal crossing-effected areas e.g. between the EU and non-Schengen BCPs or in their proximity areas. This may affect both ordinary passengers and vehicle lanes at the BCPs but also intra-border train stations. Within the last 3-4 years, this phenomenon presented a dramatic surge due to the political situation in the Middle East and Africa. Most of the illegal immigrants are trying to cross the borders hidden inside vehicles or mostly containers in trucks and train wagons, employing imaginative methods in the majority of the cases.

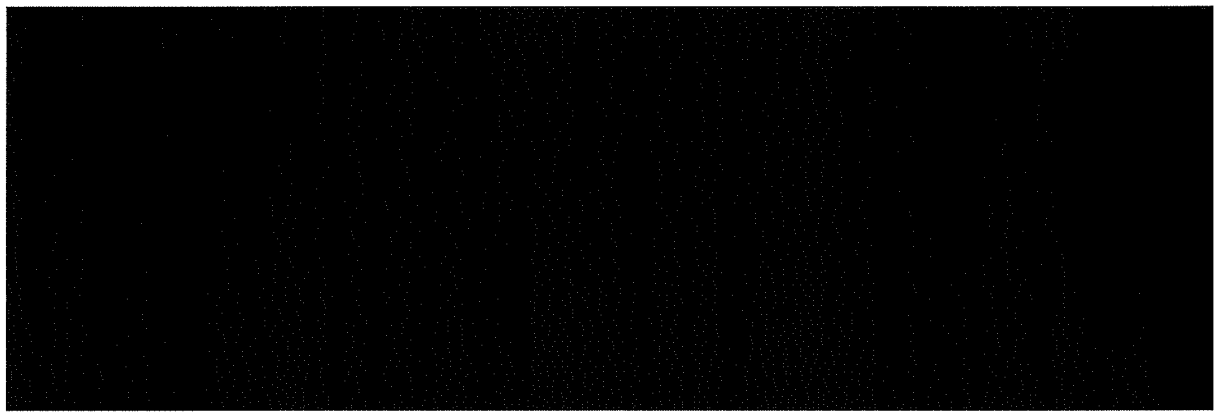
Various examples can be reported; however, it should be noted that in the majority of the cases the countermeasures require high-tech or sophisticated equipment which is not the case for all the BCPs between EU and non-Schengen countries.

For instance, considering the [redacted] Border Crossing Point in the Hungarian-Serbian border area, the following can be reported. In this territory, besides the many attempts of crossing the physical barrier, many of the people trying to illegally get into the Schengen-area, prefer to hide inside freight train wagons for crossing the border. Since autumn 2016, this way of "travelling" has highly spread; many irregular immigrants' groups travel on the back, bottom, bumper, container, chassis etc. of the trains, even risking their lives. This problem challenges the authorities and the border guards as it requires a separate group of freight / cargo train inspectors. Although it can be mentioned as a "new" and nowadays-actual way of illegal border-crossing, the "old methods" related to hide in trucks, back of vehicles did not decline. Local departments of HNP ([redacted] BCP) take photo and video documentation of all cases related to the above-mentioned methods and activities.



Similar kinds of problems have been reported in other Border Crossing Points, in Latvia and Greece as well. Especially, in Greece, the majority of the immigrants has been concentrated in the [redacted] BCP between [redacted] (non-EU / non-Schengen), after illegally inserted to the Aegean Sea, using the specific BCP as their pathway to the central Europe. In the last couple of years (2015-2016), Greece has faced a very severe problem of this kind both at the specific BCP and at the intra-border train station nearby.

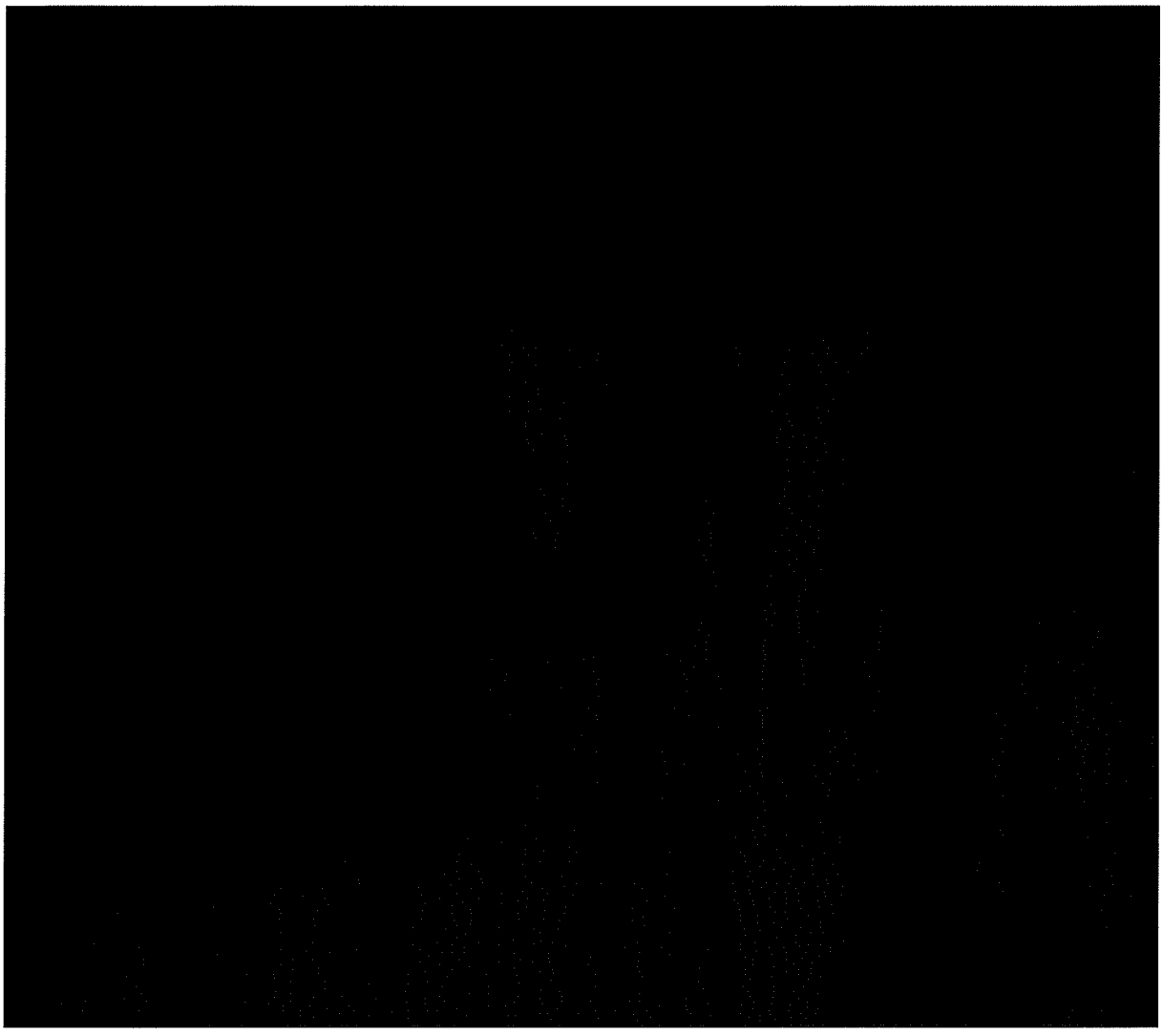
Although the severity of the problem increases nowadays, only few land borders BCPs are equipped with sophisticated equipment for the detection of hidden people or immigrants inside vehicles or containers, mainly due to economic reasons, since most of the relevant equipment is quite expensive. X-rays based methods are most reliable to detect not only hidden humans but also hidden contraband and explosives; however, they present certain disadvantages, with large and expensive installations needed being the most important one.



From the up to now overall knowledge, it should be noted that there can be no unique and single technology and relevant sensor suitable for all kinds of vehicles or closed compartments and the relevant research is still ongoing. Thus, the issue of a unique sensor which could also be portable, small in size with high level of performance for all required checks in all kinds of vehicles, still remains unsolved. Additionally, it should also be taken into account that the commercially available systems and technologies are not meant to tackle this specific problem at the BCPs but rather address a wider range of relevant applications, mainly military ones with different kinds of demands and related problems.

Taking all the above into account, it is seen that since the iBorderCtrl project attempts to provide a holistic solution to assist the Border Guards on their check controls and decisions for allowing the border crossing of all passengers (both EUs and TCNs) and in light of the current situations at the BCPs, the issue of hidden humans in vehicles needs to be addressed as well. However, up to the point that this will be feasible in terms of: a) the implementation of the relevant technologies within the procedures and processes followed at the BCPs depending on the usage scenarios and b) in view of the integration requirements and feasibility of the respective technologies with the iBorderCtrl envisioned overall system.

The above issues in terms of the technological state-of-the-art have been adequately dealt within D2.1. However, complementary to the D2.1 analysis, an assessment of the corresponding commercially available systems and solutions will be presented in the following, in order to be able to indicate what and in what degree could be used and included within the iBorderCtrl system.



6.2.1 Important additional Criteria for implementing the HHD devices

As it will be seen in the following analysis, a variety of available commercial tools exist in the market, in certain cases involving key players on the field. According to D3.1 legal assessment there is not a specific recommendation by the relevant Legal Documentation implying the mandatory use of specific devices. To this respect, all corresponding technologies and respective commercial products or even prototypes that can contribute to the detection of human presence inside vehicles or compartments need to be examined, assessed and be the pool for the selection of the implementation devices.

In many cases, commercial products foresee very sophisticated equipment meant for use strictly by the military or law enforcement agencies which might not be available for research projects. This also is the case for proprietary respective equipment. However, both may also be overqualified for the specific implementation and integration requirements of the iBorderCtrl project. To this respect, the following additional criteria for selecting the proper devices need to be taken into consideration.

Table 2 Additional Criteria for implementing the HHD devices

Characterisation of use	The devices should not be provided in a restricted manner by the respective vendors. Devices characterised strictly for military use or under special export or other license should be dealt in less priority during examination, due to the obvious fact that cannot be obtained for research purposes.
Vendor's support through EVK or SDK	Within the framework of the iBorderCtrl project, the devices for the HHD tool should enable their integration mainly in software aspects within the overall platform and system, according to the architecture and technical requirements mentioned in the previous paragraph. This means that the users should be in the position to develop their own applications through i.e. APIs from the selected devices. This presupposes the provision of Software Development Kit (SDK) or Evaluation Kits (EVK) and generally support from the vendors' side. The unavailability of this kind of support will seriously affect the final selection.
Performance	As indicated earlier, the performance of each device greatly depends on the various technologies to be implemented. In the following paragraphs the performance characteristics of each technology and respective devices will be described in detail.
Cost	Since, most of the commercially available devices of various technologies are too sophisticated or are meant for special purposes (military etc), the relevant costs might be out of the scope of the iBorderCtrl as a research project and need to be taken into account as well.

6.3 Technologies for hidden people detection

Considering continuously changing situation at European borders combined with the increasing terrorist threats across the continent, border officers and appropriate authorities need to enhance the border security through novel technologies. As described earlier, a particularly bothering trend has been observed nowadays of hidden people being illegally transported through the borders. In order to detect such practices, there are several available technologies in the market. Currently, in the majority of the cases, the relevant checks are not performed routinely, especially when traffic flow across the check points increases; instead they are made occasionally or indicatively, unless dictated by official warnings, relying mostly on visual inspection and staff's experience and perception.

In case of security sensing at border crossing points, it is important to enable border officers' remote detection of objects. The advantage of applying remote technologies is that they do not require a physical interaction/contact with the object or person of interest, to accurately detect it. These technologies can be divided into active and passive solutions. The former ones are characterized by signal transmission, which is subsequently reflected off a given object back to the sensor. The reflected signal is then collected by the receiver and the system analyses the changes in the signal reflection including the time delay between signal transmission and reception, power level, or frequency of the received signal. The latter ones, on the other hand, do not transmit any signal. Such sensors collect and process the signal generated by a given object, e.g. thermal radiation[25].

[25] Garcia, M. L., *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann, 2007, pp. 103-104

The iBorderCtrl research project will adapt existing technologies (e.g. microwave radar, heartbeat and acoustic sensors), in order to improve Hidden Human Detection techniques at European border crossing points to assist current inspection technologies. As denoted in D3.1, no specific method or tool is imposed by the respective Directives and recommendations to be used in a mandatory manner. Thus, the technologies described below, reflect the current commercially available state-of-the-art solutions that could be examined and assessed. This review will contribute to the subsequent development of the iBorderCtrl tool for hidden human detection.

6.3.1 Microwave & millimetre wave radar sensor

Since their invention during WWII, radar systems have been applied in numerous fields both military and commercial for such purposes as airplane detection and tracking, vehicle velocity measurement, topographic mapping, oil spill detection, etc. More recently, however, radar based technologies are used for security reasons including human movement and illicit goods detection, and even heartbeat and respiration detection (the last two aspects are presented in more depth in section below devoted to heartbeat detectors). Since illicit goods detection is outside the iBorderCtrl scope, the following description will focus on the detection of passengers illegally crossing the borders.

The steadily increasing number of people's illegal transportation attempts across the EU border crossing points, dictates the deployment of fast, robust and contactless solutions for detecting such practices. Currently, most of the available technologies and scanners, utilize x-rays in order to penetrate the target object. Such technologies (discussed in more detail in the next section), are considered to be harmful for human health since they generate ionising radiation. Moreover, commonly used scanners are, in most cases, expensive standalone tools/gates of considerable size addressing mainly cargo scanning purposes. Thus, alternative solutions are required, which will be characterized by lower cost, portability, and little intrusiveness for travellers.

Before proceeding, a brief explanation of radar operating principles will be provided. A radar is a device made of a transmitter that generates electromagnetic waves as well as a transmitting and receiving antenna (often one antenna performs a dual function), which detects the echo of the reflected electromagnetic wave[26]. Basically, the electromagnetic radiation is applied to detect objects. Depending on the applied wavelengths, radars can penetrate various types of materials. For the specific application, radars based on the Doppler effect principle are particularly interesting and these are basically used in practice. In general, the Doppler effect is a shift in the frequency which is the result of reflecting wavelengths on a moving object. When the object is moving towards the radar device, the frequency is steadily increasing and when the object is moving in the opposite direction to the radar, the frequency is gradually decreasing[27]. Figure 20 below illustrates the effect. The red dot represents the source of the signal, while the circles around it are the signal waves. The sinusoidal lines are representing the frequency of the signal wave.

[26] Hall, Peter S., Hall, and Peter S. "Antennas and Electromagnetic Wave Propagation: Radar, Seekers and Sensors, Tracking, and Target Recognition.", Encyclopaedia of Aerospace Engineering. John Wiley & Sons, Ltd, 2010.
[27] Petrescu, Florian Ion. A New Doppler Effect Germany 2012. Books on Demand, 2012.

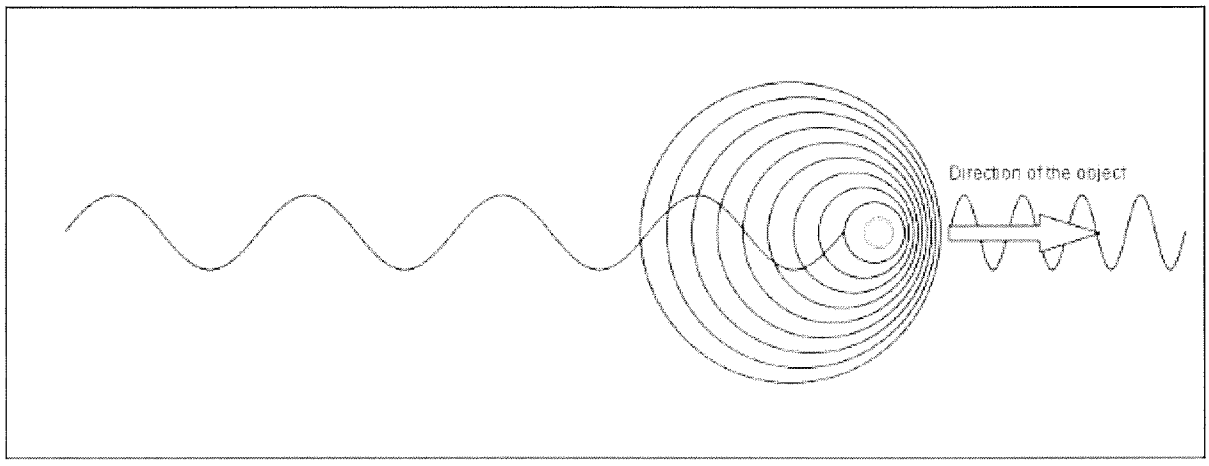


Figure 20 Doppler Effect

In case of hidden object or human detection, radars operating in microwave and millimetre-wave lengths of electromagnetic spectrum are particularly effective and have numerous advantages compared to other technologies. The microwave spectrum ranges from 3 GHz up to 30 GHz, whereas the millimetre-wave band extends from 30 GHz to 300 GHz. According to the rules defined by the International Telecommunication Union (ITU), microwave and millimetre-wave frequencies fall into categories of super high frequency (SHF) and extremely high frequency (EHF) in the ITU spectrum. Both microwave and millimetre-wave bands are also denoted by IEEE letters. The former is said to range from S-band up to K_a-band. The latter, on the other hand, extends from K_a-band up to a millimetre-wave band not denoted by standardized letter. The full IEEE letter designations is as follows: HF 3-30 MHz, VHF 30-300 MHz, UHF 300-1,000 MHz, L-band 1-2 GHz, S-band 2-4 GHz, C-band 4-8 GHz, X-band 8-12 GHz, K_u-band 12-18 GHz, K-band 18-26,5 GHz, K_a-band 26,5-40 GHz, V-band 40-75 GHz, W-band 75-110 GHz and mmw 110-300 GHz[28].

Through the application of microwave or millimetre-wave bands, there are numerous benefits that can be achieved in terms of security. Namely, such radar devices use the frequencies which propagate with little attenuation across the atmosphere. Furthermore, they may easily pass through clothing, luggage, even some building material with minimal attenuation, which renders these devices appropriate for hidden object detection. Radar systems are also vital solutions for contactless hidden human detection by exploiting the Doppler shift principle. Yet another advantage of contemporary radar systems is that the prices of radar components are gradually decreasing, which make them affordable for a wider range of customers.

Highly sophisticated imaging systems, for example for military through-the-wall-sensor applications, combine the basic Doppler principle with multifrequency radar systems for detecting humans and classifying their activities at short and long ranges. Short-range radar systems of this kind operate at lower frequencies (i.e. the S-Band) for through-wall applications at distances of up to 3 m, utilizing a wide-band noise waveform or a continuous single tone. The long-range ones operate in higher millimeter-wave frequencies (i.w. even W-Band) for distances of up to about 100 m in free space and up to about 30 m through light foliage; they employ composite multimodal signals consisting of two waveforms, a wide-band noise waveform and an embedded single tone, which are summed and transmitted simultaneously or utilize ultra-wide band relevant technologies. Matched filtering of the

[28] Nanzer, Jeffrey. 2012. *Microwave and Millimeter-wave Remote Sensing for Security Applications.* Boston: Artech House, pp. 7-8.

received and transmitted noise signals is performed to detect targets with high-range resolution, whereas the received single tone signal is used for the Doppler analysis. Doppler measurements are used to distinguish between different human movements and gestures using the characteristic micro-Doppler signals[29]. Millimetre (mm-) wave passive and active imaging offers rapid remote detection of metallic and non-metallic objects and contraband concealed beneath clothing, enabling "through-the-wall imaging systems (TWIS)" and humans' remote observation for military and law enforcement personnel, but not through metal walls.

Nevertheless, it is evident that detection of people hidden inside steel-walled containers is difficult with radars since the wall is made of metallic material, which severely attenuates the transmitted electromagnetic signal. Neither microwave, nor millimeter-wave radars are able to properly penetrate thick steel or concrete materials in order to detect human presence. In this respect, x-ray scanners seem to have an advantage over radar systems[30].

6.3.2 X-ray scanners

Amongst the techniques dedicated to contraband and hidden people detection, tools that use X or Gamma rays, are particularly effective. The prevalent solution, which is based on such technology, is a radiographic x-ray imaging device. The device emits either a single X-ray wide area shot or is continuously generating x-ray bands on the object in a linear and narrow manner. Radiographic X-ray imaging comprises such solutions as checkpoint screening of small objects/luggage, computed tomography (CT) scanning of objects for explosives detection, X-ray backscatter for detection of hidden objects carried by persons, and high-energy screening for detection of contraband and hidden people inside cargo containers, vehicles, trains, etc.[31]

Application of CT for luggage screening has been based on medical applications of CT scanning. Computed tomography, which is often described as an extension of radiography, takes a series of images with an area detector or a linear array projection from various angles around the target object. Subsequently, the images are merged, in order to reconstruct the X-ray attenuation of objects in the luggage. The application of CT screening tools at border crossing points is mostly attributed to the superior effectiveness in explosives and illicit objects detection. The advanced CT screening tools are distributed by L-3/ANALOGIC, AS&E, Leidos, Smiths/Heimann, Rapiscan and a few other suppliers[32]. Current statistics indicate a continuous growth in the application of CT screening, especially at major airports. The technology has advantage over older 2D X-ray imaging solutions since state-of-the-art 3D CT screening tools allow to extract a clearer image of the luggage contents without the need to take out all the electronic devices[33]. The example of computer tomography screening image is presented in Figure 21.

[29] RamM. Narayanan, Sonny Smith, and Kyle A. Gallagher, "A Multifrequency Radar System for Detecting Humans and Characterizing Human Activities for Short-Range Through-Wall and Long-Range Foliage Penetration Applications" International Journal of Microwave Science and Technology Volume 2014 (2014).
[30] Mery,D., Computer Vision for X-Ray Testing: Imaging, Systems, Image Databases, and Algorithms, Springer, 2015
[31] Mery,D., *Computer Vision for X-Ray Testing: Imaging, Systems, Image Databases, and Algorithms*, Springer, 2015
[32] Billie H. V., *Bombers, Hijackers, Body Scanners, and Jihadists*, Xlibris Corporation, 2012
[33] http://www.airport-world.com/news/general-news/5582-singapore-changi-trialling-new-computed-tomography-ct-security-screening-technology.html (accessed: 06.06.2017)

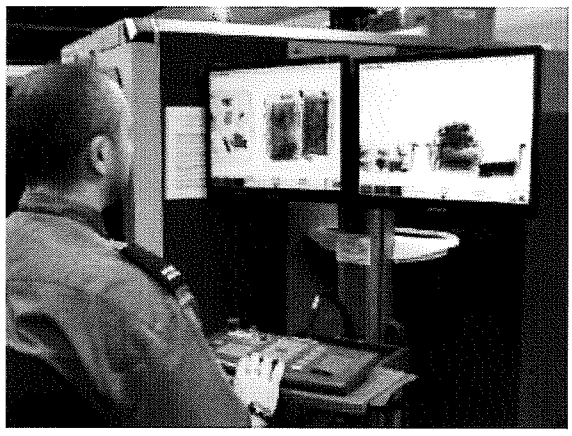


Figure 21 CT screening using Rapiscan solution (source: www.rapiscansystems.com).

As numerous border authorities put premium on novel security and screening solutions, X-ray backscatter body scanners seem to attract a lot of attention. X-ray backscatter projects low radiation X-rays on a person standing in the screening portal. Subsequently, the scanner detects the X-rays reflected from a given person, in order to reveal hidden items, which are characterized by low Z materials. Low Z materials (materials with low atomic numbers), scatter the X-rays (e.g. explosives with nitrogen). Higher Z materials cause less X-ray backscatter. The sensor can also detect the lack of scattering. Thus, such a sensor can detect objects characterised by high Z material (objects which absorb X-rays). Figure 22 below illustrates an image generated by the system at the user's interface[34].

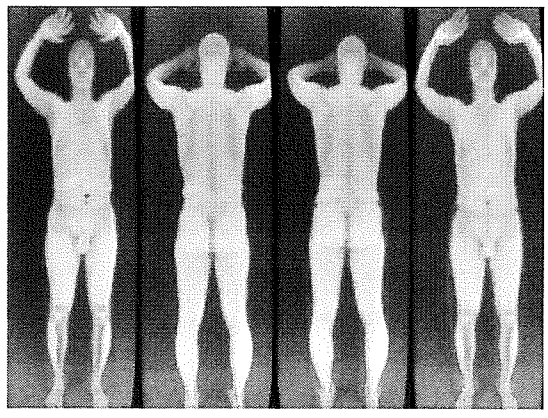


Figure 22 Image generated by X-ray backscatter body scanner (source: wired.com).

Yet another type of X-ray imagers, as mentioned above, are the high energy X-ray screening tools used for contraband and hidden human detection inside cargo containers. These devices are also known as unit load devices (ULDs). Such tools are designed to penetrate thick steel cargo containers and vehicles to reveal any concealed objects or persons. Oftentimes, devices equipped with lower-energy X-rays turn out to be insufficient to penetrate the target objects. Devices, whose energy output is limited to 450 KeV (kilo-electron-volts) allow only to penetrate 100 mm of steel. However, the tools based on X-rays with linear accelerators with energy output reaching 9 MeV (mega-electron-volts) are capable of penetrating 400mm of steel, what renders them sufficient for cargo inspection.

[34] Klitou D., *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Springer, 2014

Nevertheless, it needs to be acknowledged that the application of such solutions is connected with high radiation levels on the target object[35].

Having considered the above, X-ray imagers offer superior effectiveness with regard to illicit goods and hidden human detection. Nevertheless, for the scope of the iBorderCtrl project, X-ray imagers seem to be at a disadvantageous position. There are numerous drawbacks, which basically exclude the possibility of using X-ray technology for the HHD tool. Namely, the X-ray tools, though effective, are very expensive. Furthermore, over the recent years, there have been numerous concerns and complaints regarding the impact of X-ray radiation on human health. Moreover, it has been reported that backscatter body sensors not only expose people to a harmful level of radiation but also may invade privacy rights of citizens. Therefore, X-ray imagers are not recommended for further research in the iBorderCtrl framework.

6.3.3 Acoustic sensor

Another technology that can be used for hidden human detection is acoustic sensing. Acoustic sensors are devices capable of detecting acoustic waves passing through solid bodies or air along with metal walls. This technology can be either passive or active (the difference between active and passive sensors was described in the previous section)[36].

Acoustic sensors can operate at different frequencies:

- Infrasound (infrasonic) – less than 16 Hz;
- Sounds which are audible by humans (sonic) – about 16 and 20 kHz;
- Ultrasound (ultrasonic) - more than 20 kHz;

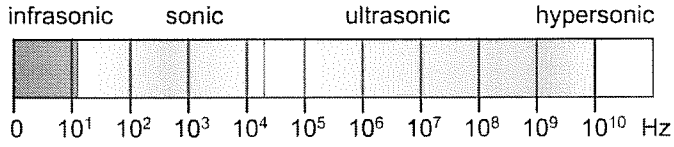


Figure 23 Sound wave spectrum (source: sengpielaudio.com)

From the above it is derived that sensors operating at the sonic and the ultrasonic ranges, can be applied to hidden human detection.

Ultrasounds are sound waves above human hearing threshold – their frequency exceeds 20kHz. Ultrasounds are commonly used, for example in maritime sonars (devices used for mapping and detecting underwater objects). Nowadays, sonars are adapted to operate in environments other than the underwater one. For example, ultrasound sonars are commonly used in basic mobile robots for navigation and object detection (distance measurement) and for medical purposes too, as the ultrasound imaging can provide a means to obtain images of the interior of the human (or animal) body. Ultrasounds are also commonly used in motion sensors – the devices for human detection and/or automatic door opening mechanism.

There are many types of acoustic sensors available, from which the following can be listed: classic microphones, fiber-optic based and MEMS (MicroElectroMechanical System) sensors. Novel microphones can be very sensitive and can be used for many different applications, for example, in

[35] Reed, W A., *X-ray cargo screening systems: the technology behind image quality*, Port Technology International, PT35-13-1, pp. 1-2

[36] http://www.wikid.eu/index.php/Acoustic_sensor

the field of audio recording, voice recognition and various scientific applications[37]. Fiberoptic-based acoustic sensors convert the optical signal (light) to an acoustic one. MEMS based acoustic sensors are small and portable devices which can be easily connected and combined within an electronic system, for example, in mobile robots. A MEMS acoustic sensor is a device that is pressure-sensitive and can convert acoustic waves to electrical signals[38]. Also, high-power acoustic sensors are reported based on narrowband mechanical-impact acoustic transmitters and matched resonant receivers, producing high-power acoustic pulses at one or more discrete frequencies[39].

Research related to human breath detection[40] shows that using microphone, human breath can be detected and measured. Unfortunately, detection based on microphones and hearable frequencies does not provide 100% accurate human detection. Nevertheless, acoustic sensing technologies combined with other technologies, related to the hidden human detection, can provide adequate results.

6.3.4 Heartbeat detectors

Heartbeat detectors are basically acoustic sensors like geophones; however, due to their specific use, are considered herein as a separate category.

Quite recently, novel systems (called heartbeat detectors) for hidden human detection have emerged. They have been designed to perform fast and effective border checks of cargo containers and lorries at border crossing points. Usually, a heartbeat detector is a complex system that comprises several sensors based on different types of technologies, which complement each other and allow to accurately detect human presence. Usually, a heartbeat detector consists of geophones (seismic sensors), acoustic sensors, as well as state-of-the-art algorithms for signal processing. Heartbeat detection often constitutes an alternative to X-ray scanning or gas concentration measurements as the latter may not always be applied in practice. Moreover, heartbeat detection offers a non-invasive detection that does not exert negative effects on human health. Based on all the above, geophones and similar kinds of heartbeat detectors may be considered as part of the wider acoustic sensors family solutions.

6.3.5 Gas sensors

Research on novel sensing techniques has provided new, different technologies based on chemical reactions such as redox, oxidation or fluorescence. The size of the devices also changes with the technology advancements. For laboratories and static research applications, large standalone sensors based on mass spectrometry or spectroscopy are used. On the other hand, some of the gas sensors are of the nano-scale (e.g. carbon nanotube-based sensors that have a size between 1 to 100 nanometres)[41].

[37] http://www.sensorsmag.com/components/acoustic-wave-technology-sensors
[38] https://link.springer.com/content/pdf/10.1007%2Fs13320-014-0148-5.pdf
[39] Felber, F, "Demonstration of novel high-power acoustic through-the-wall sensor" Proc. SPIE 9456, (2015).
[40] http://www.cs.rug.nl/~aiellom/tesi/avalur
[41] Zaporotskova, Irina V. et al., *Carbon Nanotubes: Sensor Properties. A Review,* Modern Electronic Materials, 2016, pp. 95–105

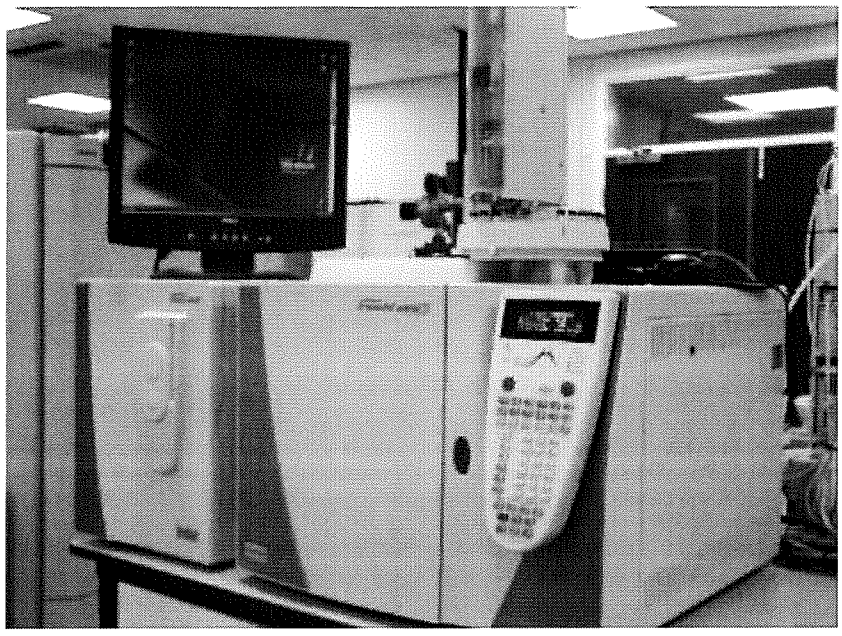
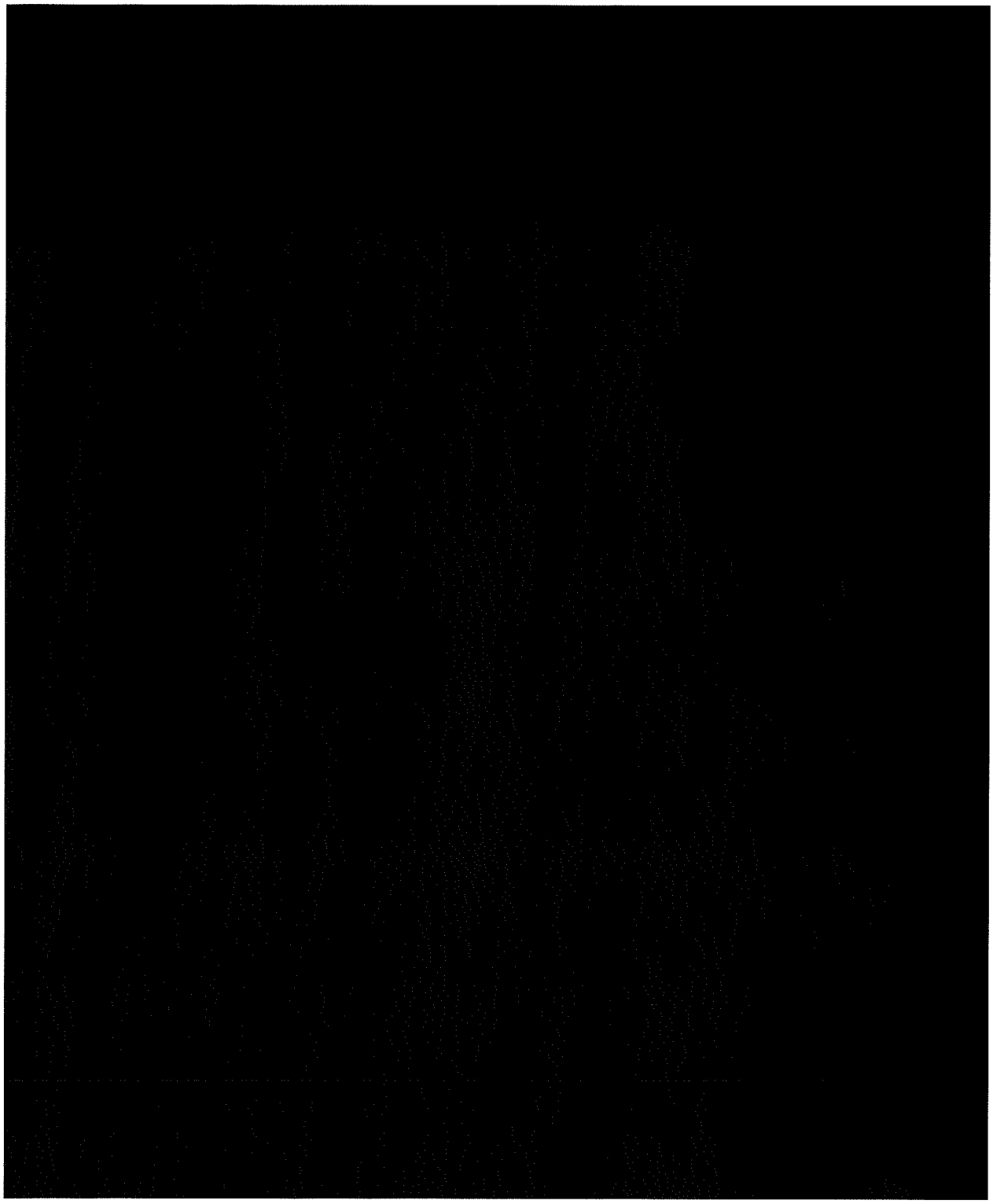
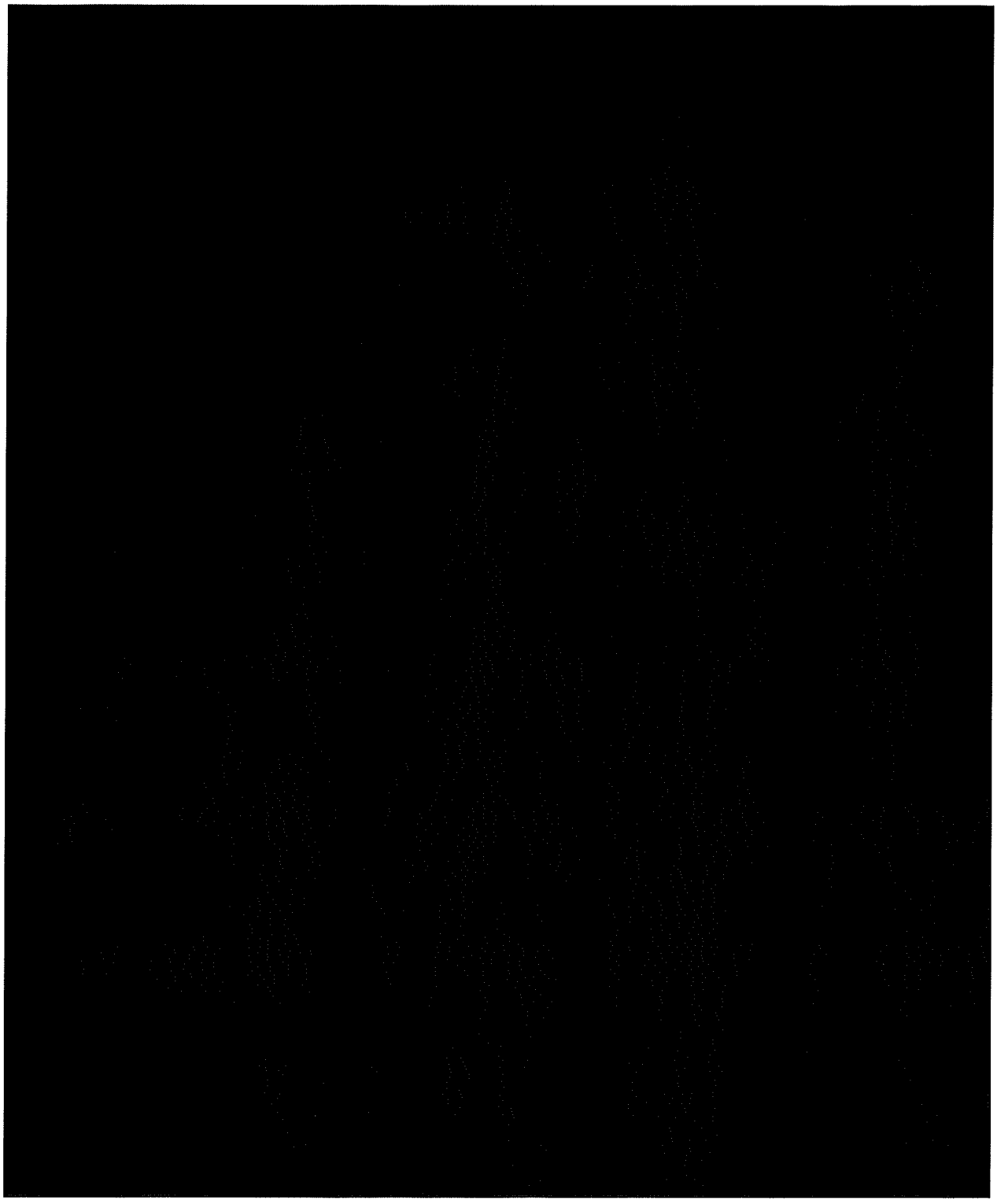


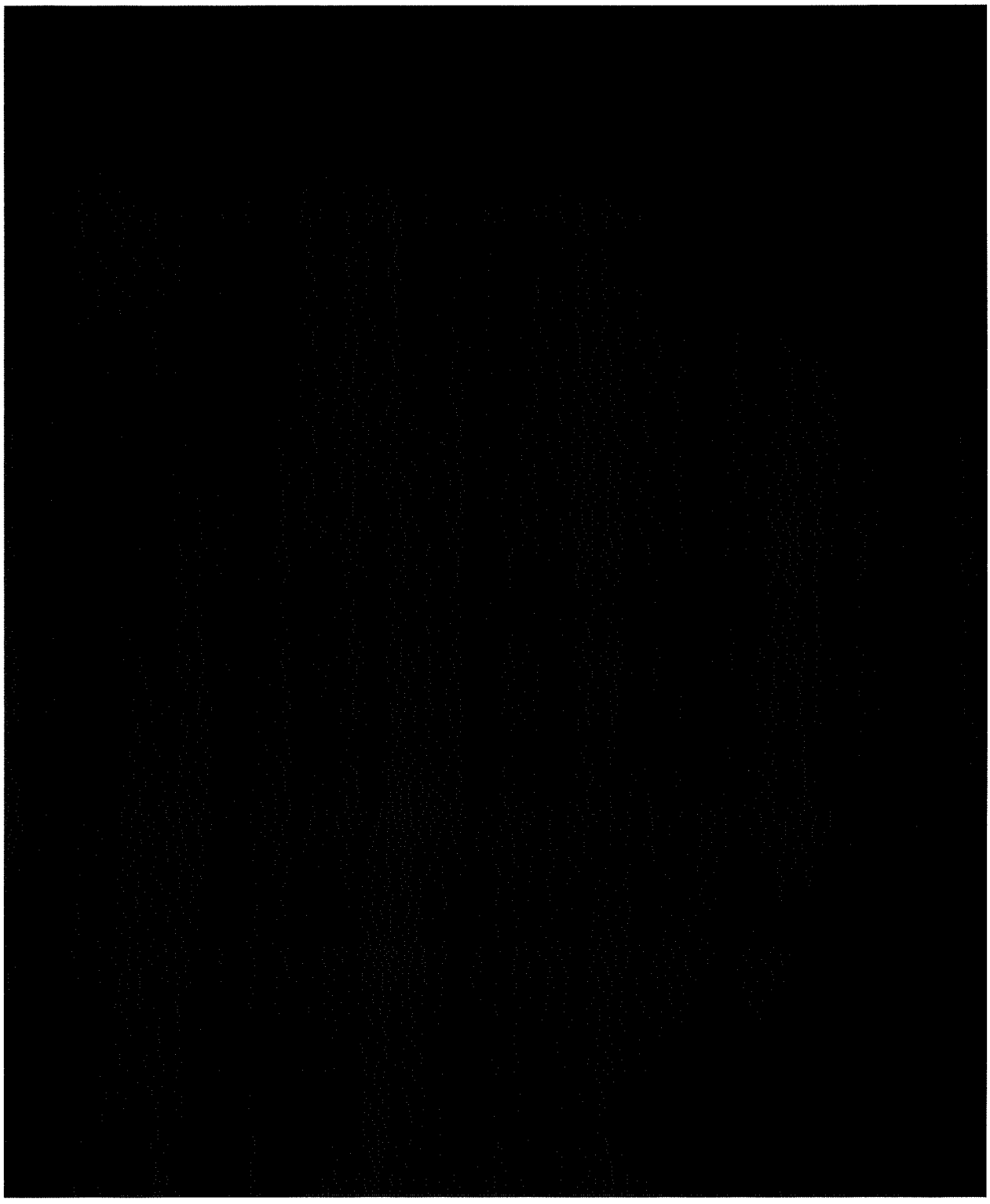
Figure 24 Mass spectrometer[42]

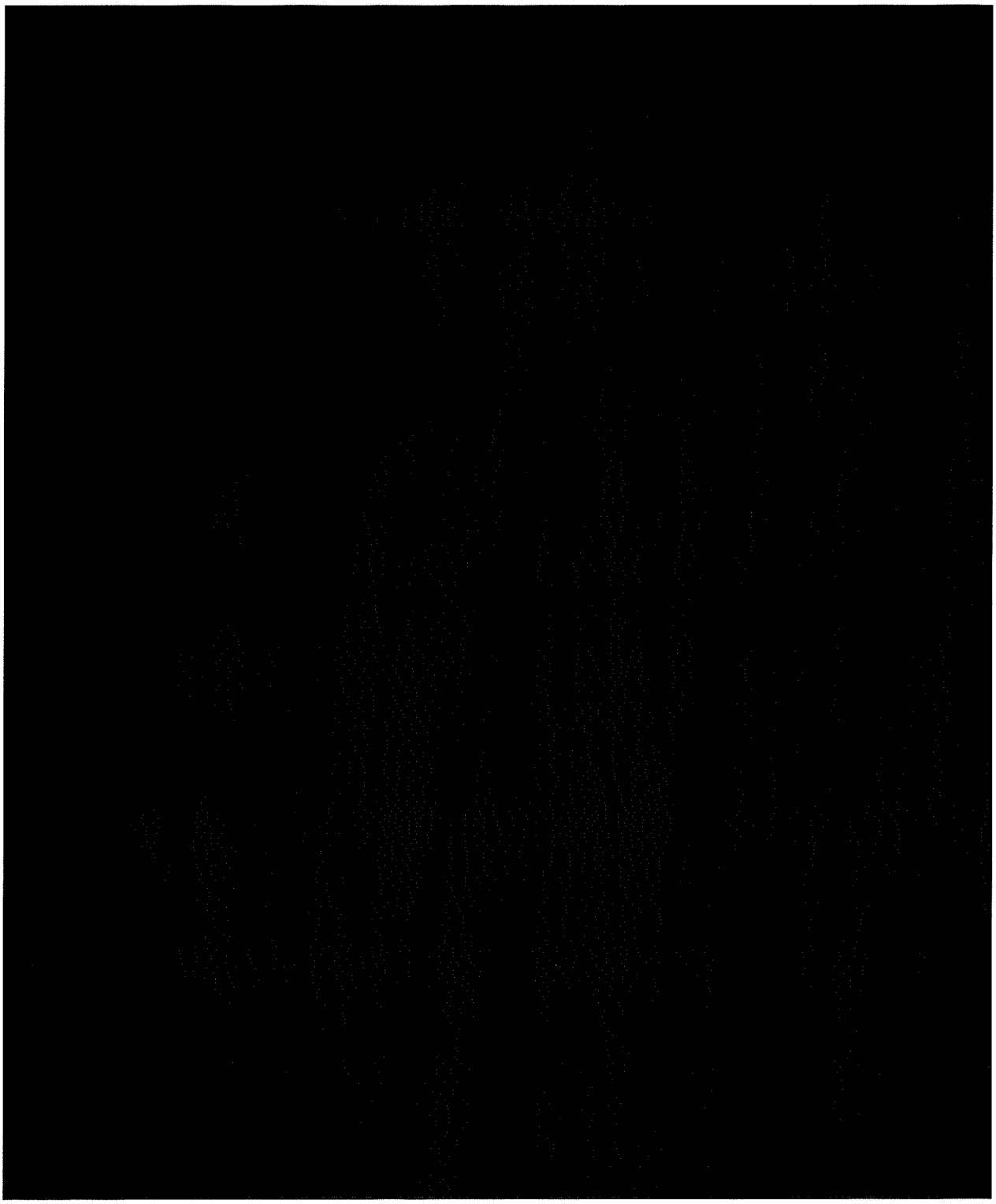
There are many types of gas sensors capable of detecting various gases. For example, there are devices that can detect substances such as carbon dioxide (CO_2), carbon monoxide (CO), oxygen (O_2) or volatile organic compounds (VOC)[43]. An exemplary technology that can be used for gas sensing, is the nondispersive infrared (NDIR). Sensors made using this technology, are able to detect carbon dioxide, with a sensitivity of 400ppm[44]. Another type of gas sensor is the Metal Oxide Semiconductor, which is based on oxide reactions. Devices of this technology are usually low cost and have a high sensitivity. For hidden human detection applications, carbon nanotubes[45] based sensors seems to be the technology of choice. These sensors can detect even extremely small quantities of gases.

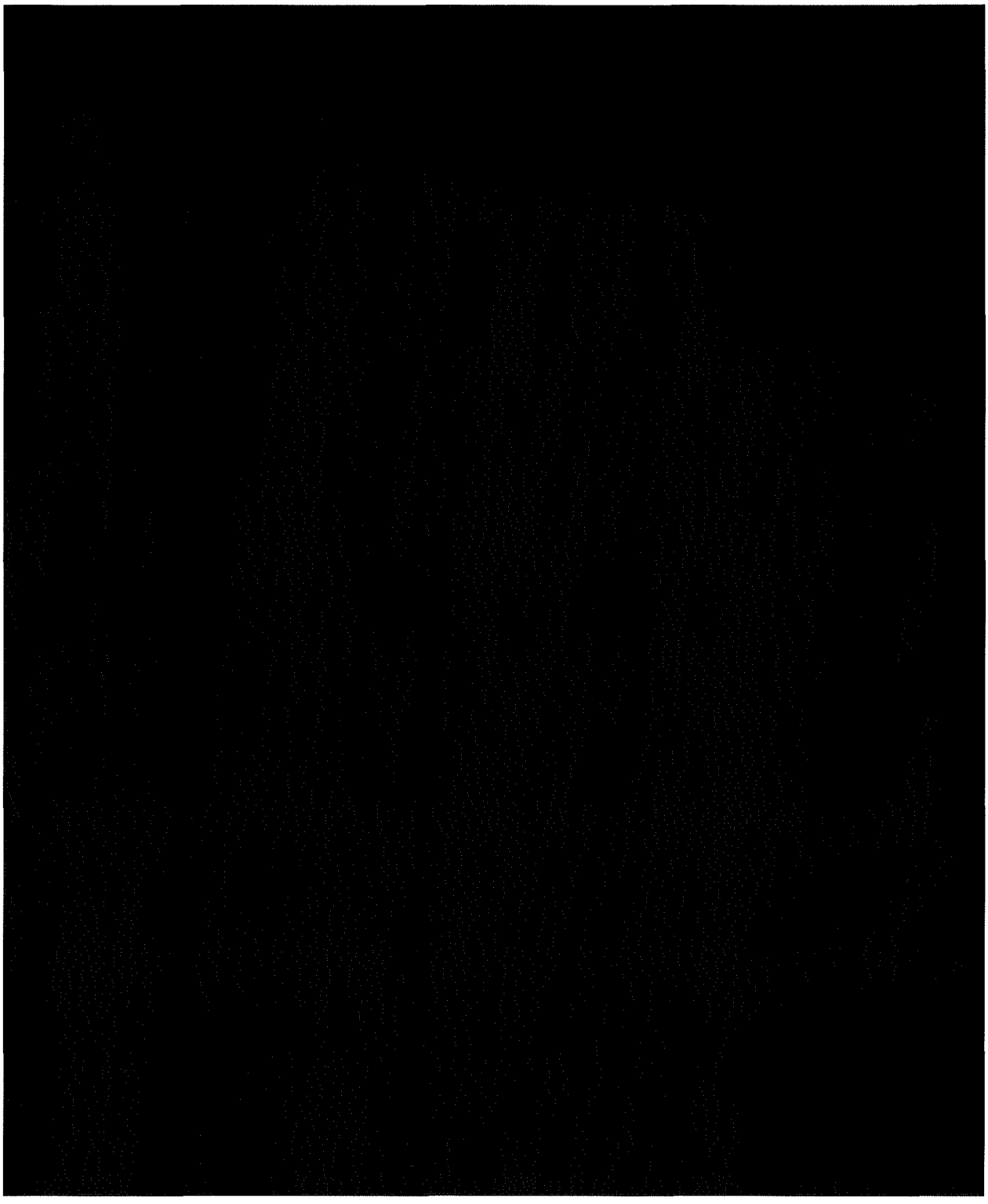
In general, sensors capable of measuring CO_2 and/or O_2 level can be utilized for detecting hidden humans in vehicles. If a person hides in a vehicle, the level of CO_2 will raise (and the level of O_2 will decrease). Consequently, if a sensor can accurately measure and track the concentrations of these two substances, the acquired data can be used to tell if someone is hiding in a vehicle.

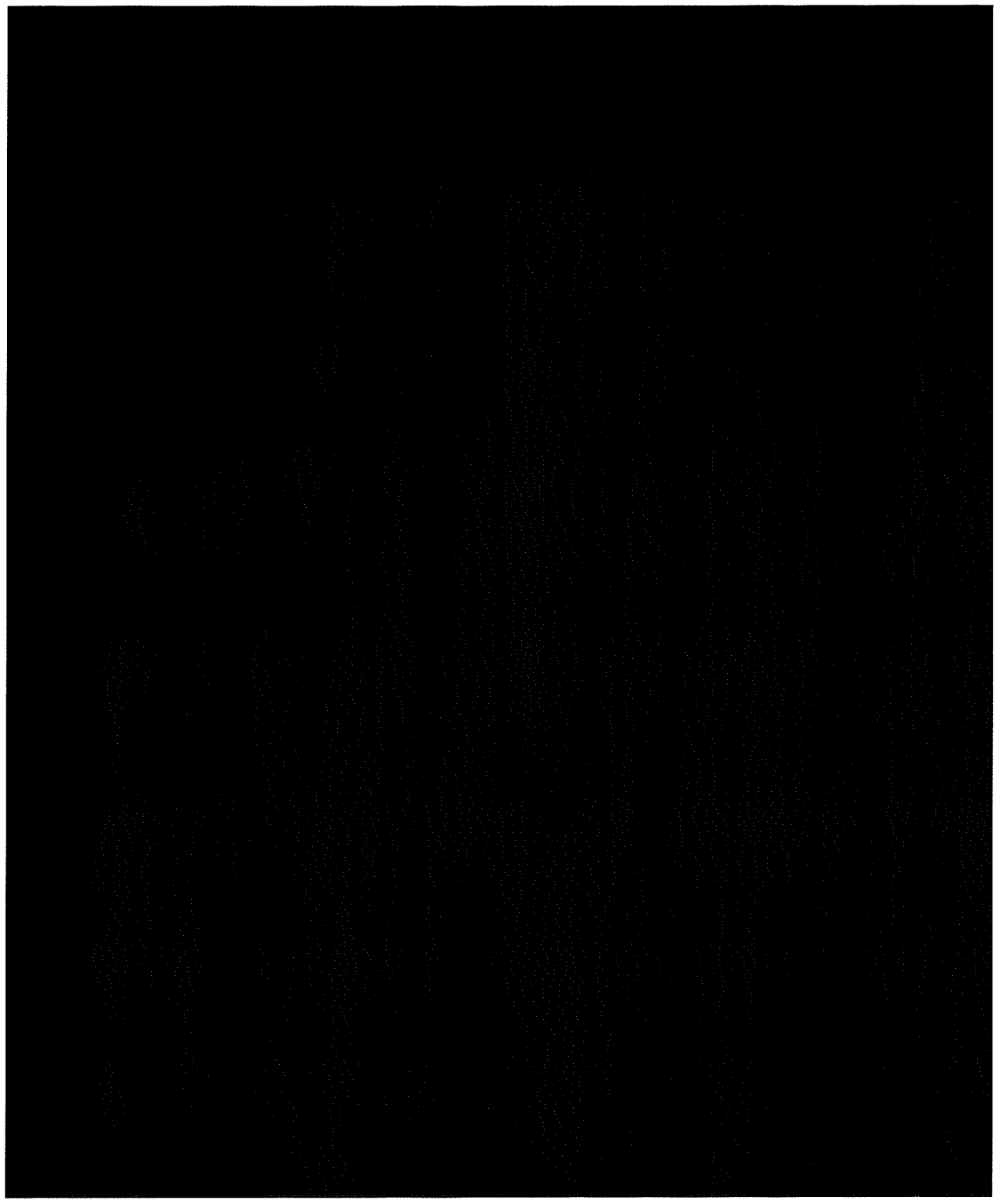


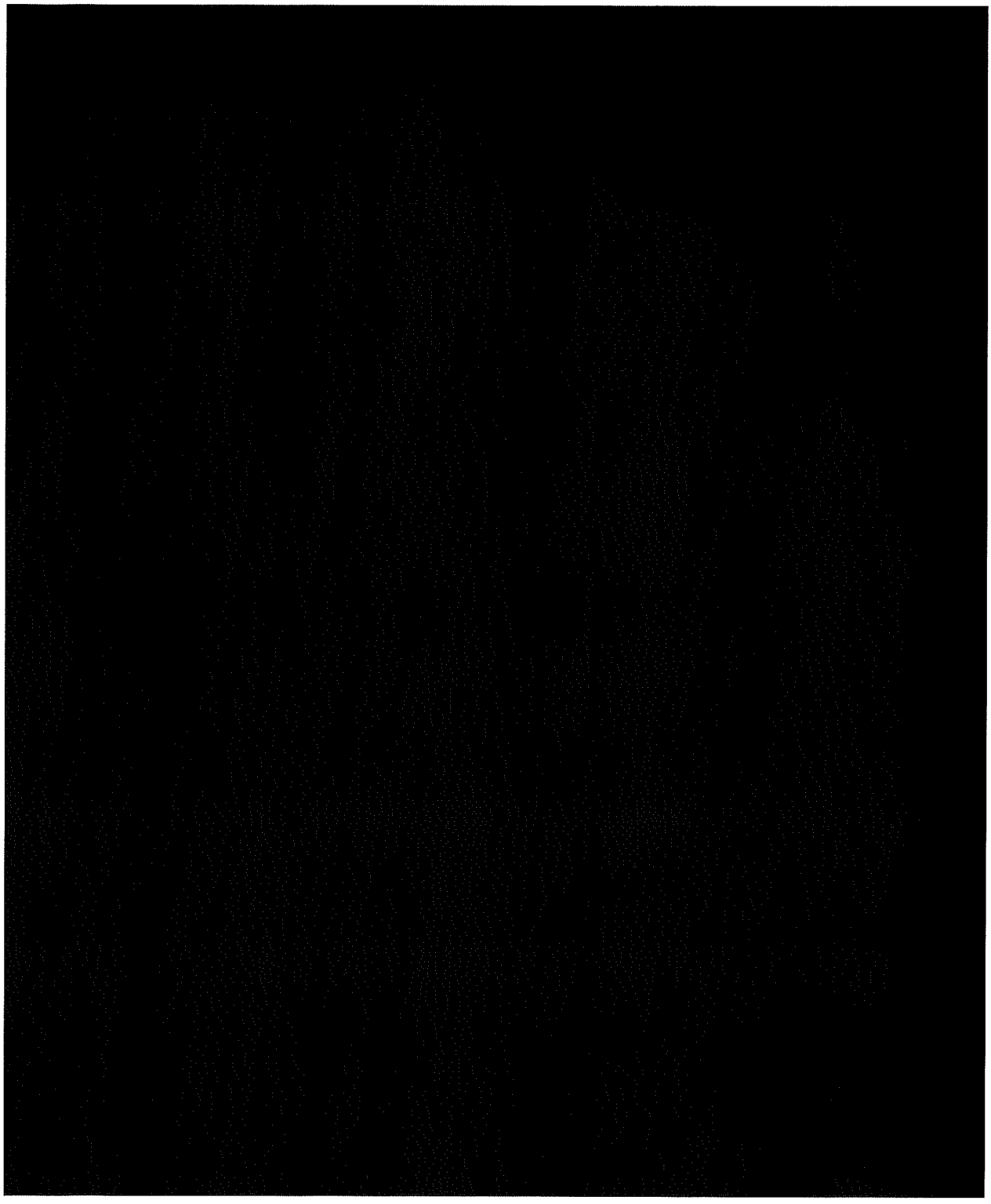


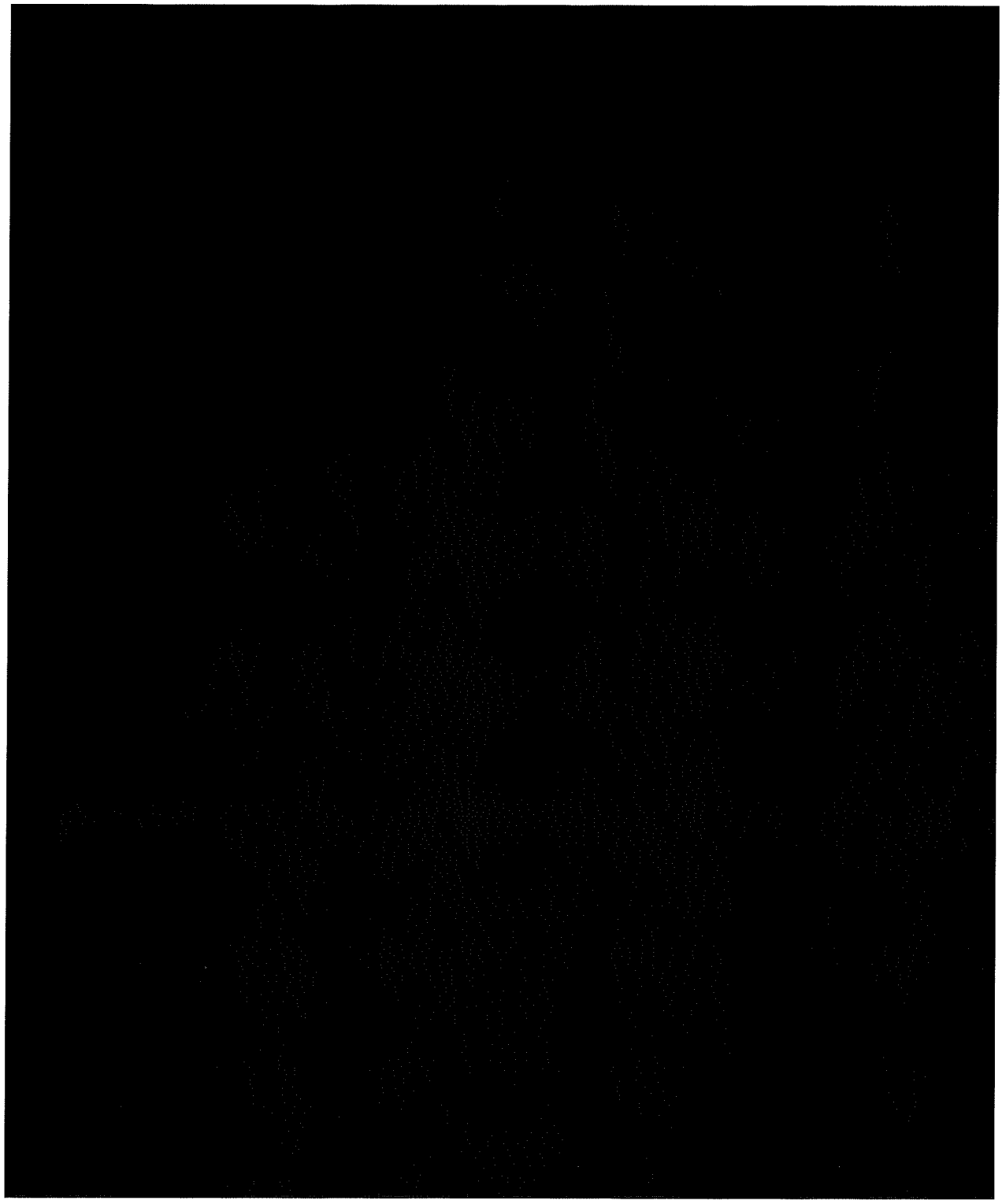


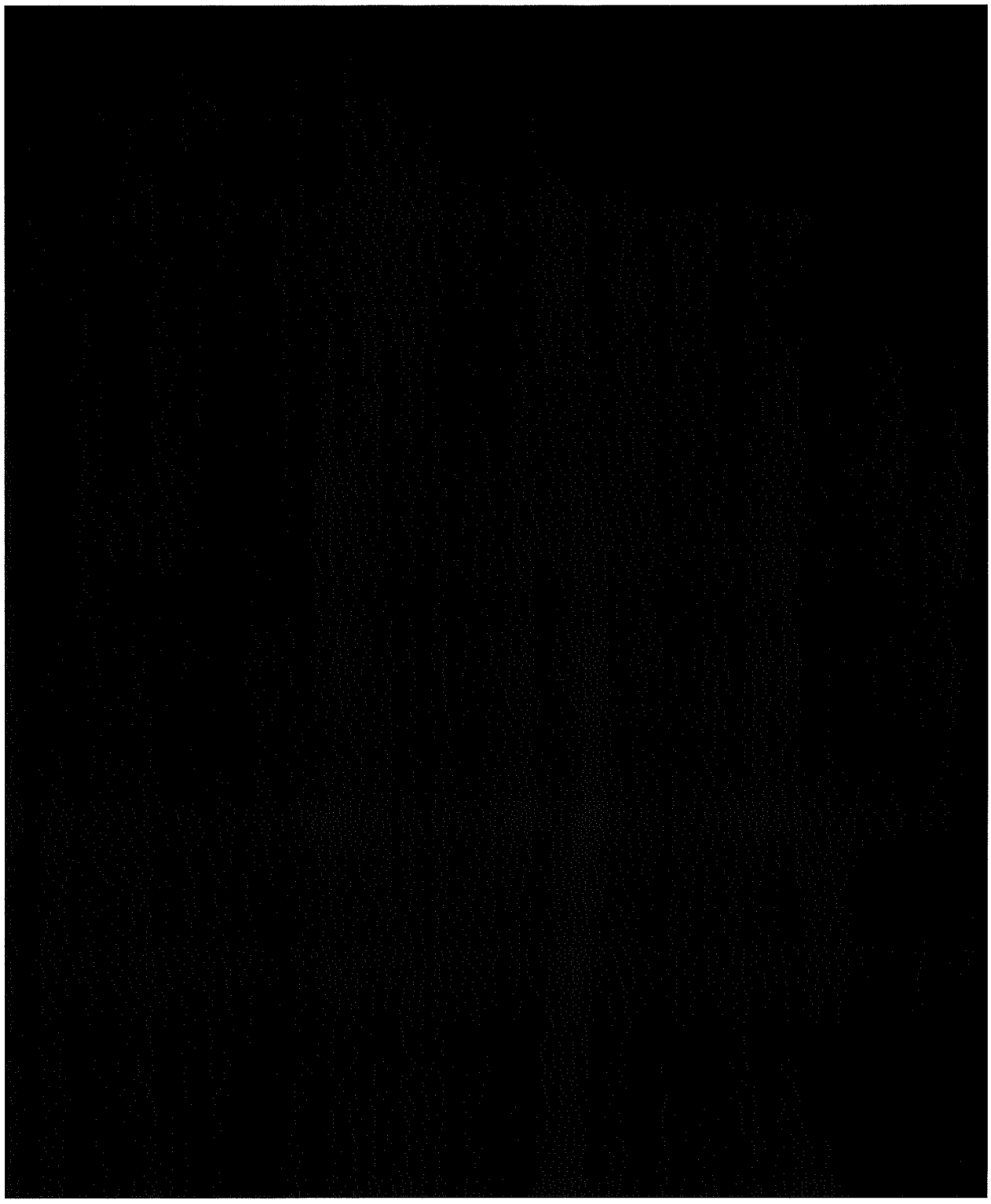


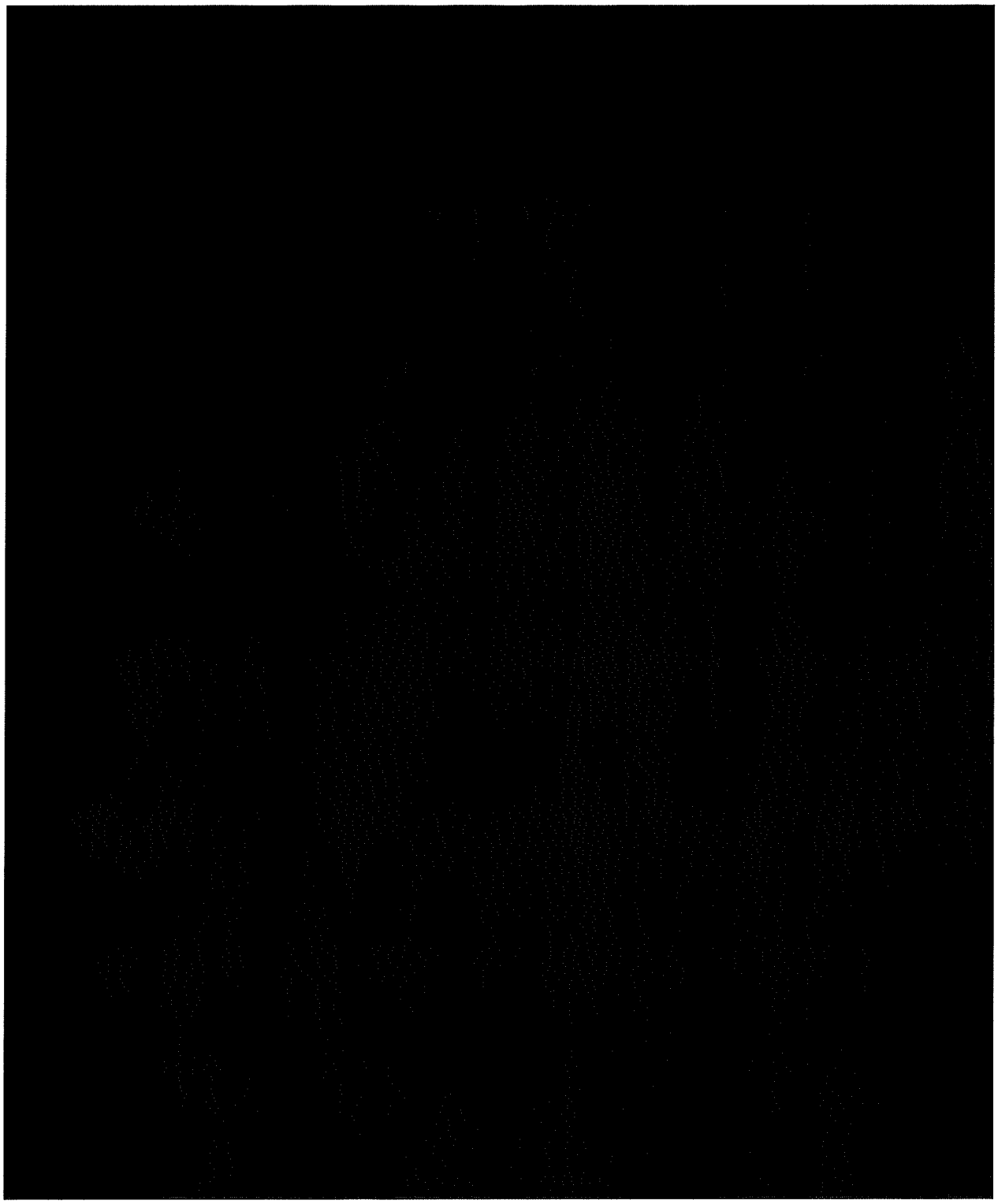


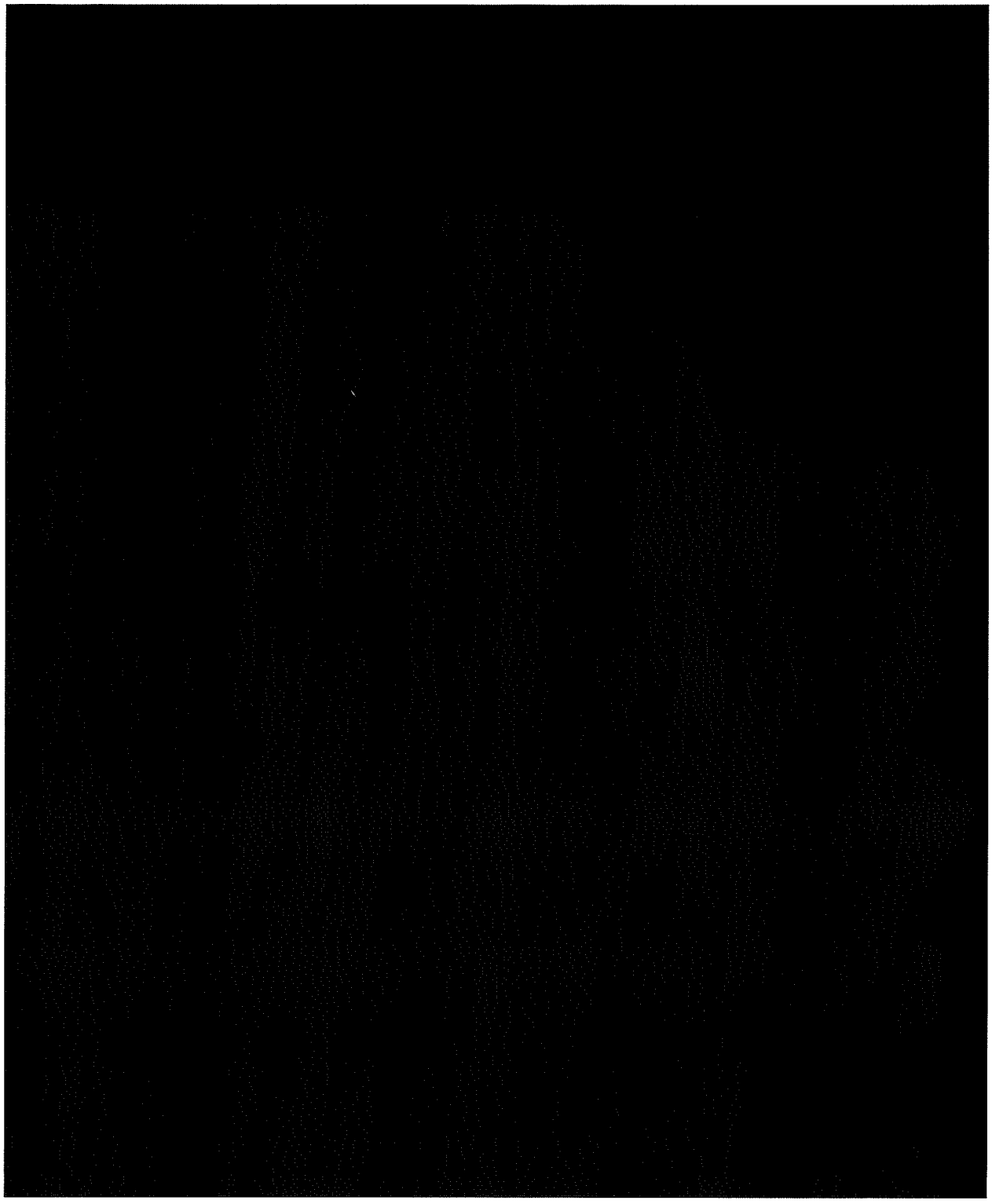


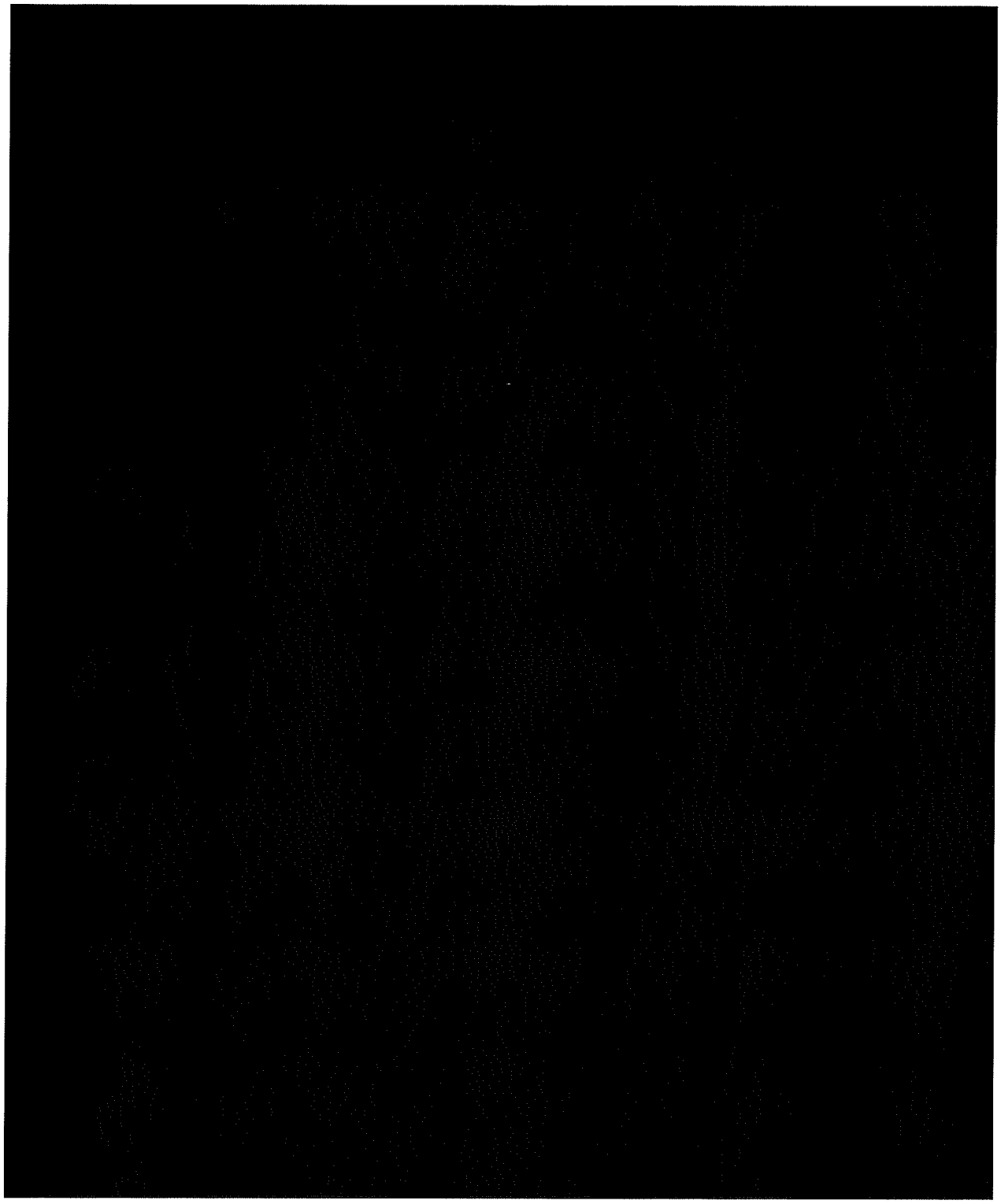


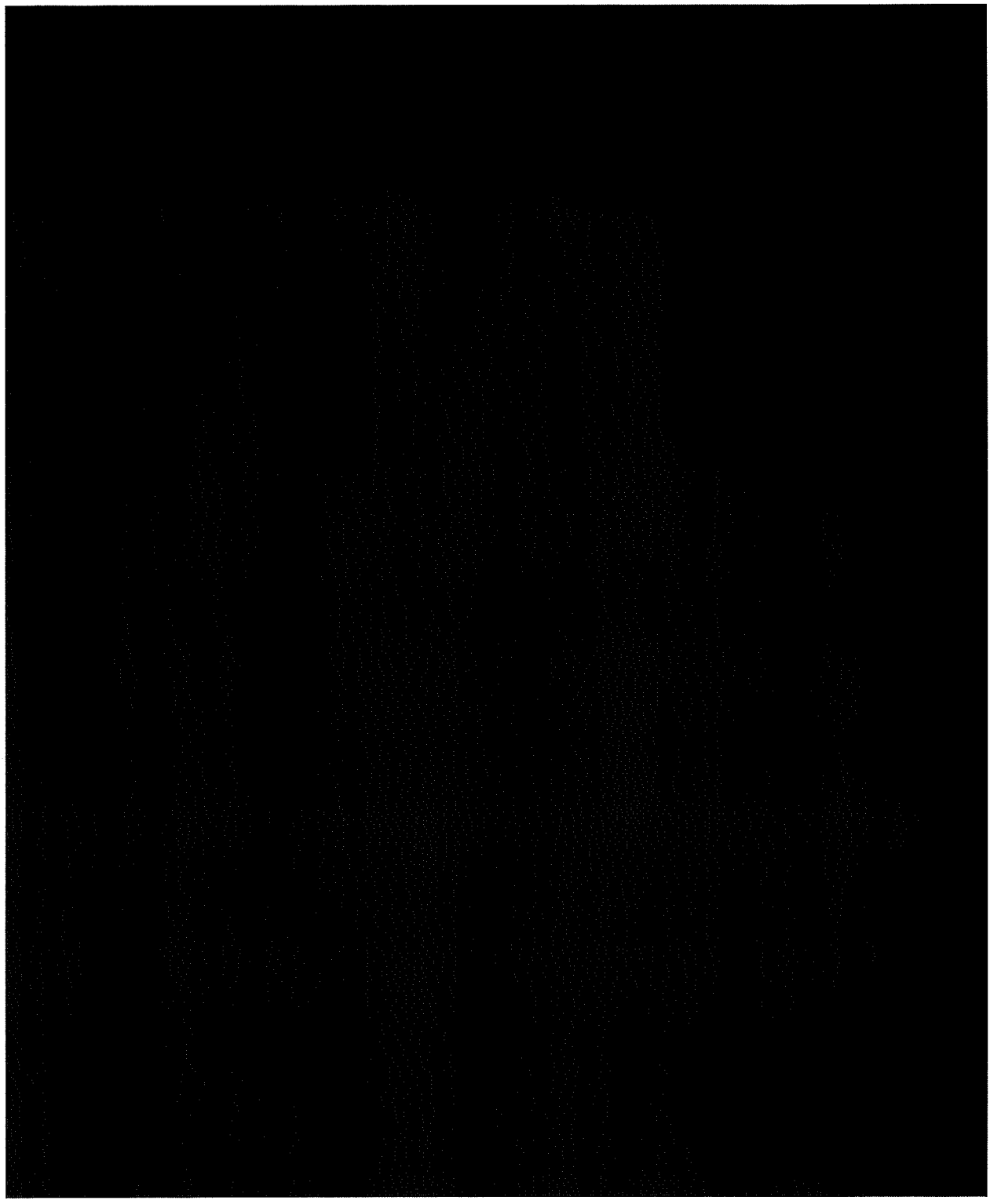


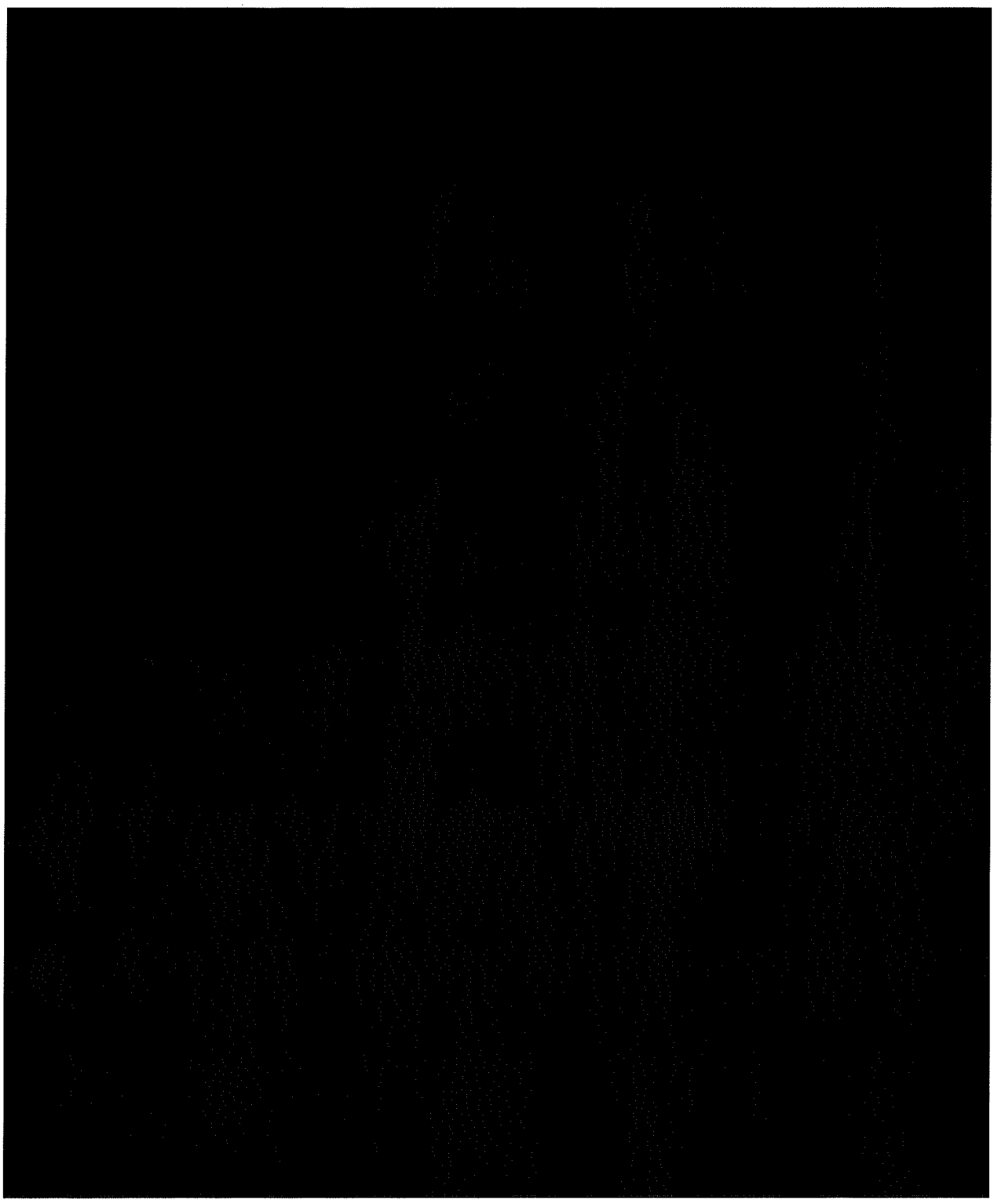


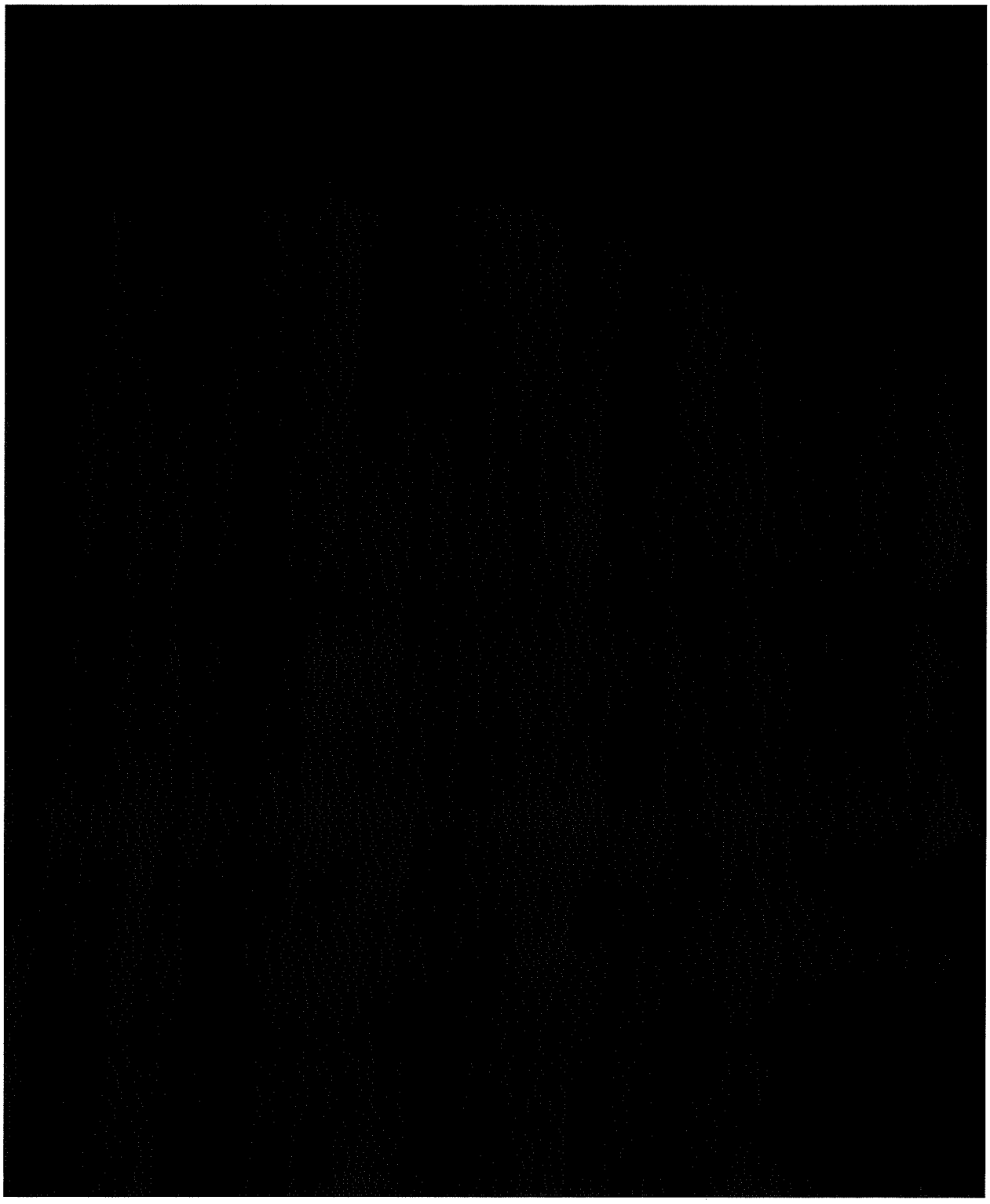












6.4 Sensors for HHD tool selection

6.4.1 Tool description

The sole purpose of the Hidden Human Detection (HHD) tool is to support the border guards in detecting passengers illegally trying to cross the border, hiding in cargos (containers, freight trains etc.) or vehicles. The key requirements of such tool (as indicated in D2.2) concern its connectivity to the iBorderCtrl portable unit, portability, relatively small size and possibility of integration with the iBorderCtrl platform according to the relevant iBorderCtrl requirements. The HHD module shall include different sensors based on the technologies examined and assessed in the previous sections of this chapter, along with the relevant analogue and digital processing units to enable data acquisition and signal processing.

The HHD tool will be connected via USB or Bluetooth to the portable computer (laptop / tablet) of the Portable Unit and will support operation on Microsoft Windows. Due to the sensors foreseen, the HHD tool cannot be mounted to a wearable device (the sensors cannot be mounted). The sensors to be used should be harmless for human beings.

The HHD tool will provide to the Border Guard User Application, an event including a score on the detected presence (or not) of a hidden alive being inside the vehicle. The score is ideally a "go / no go" action. However, a probability index of presence detection will be included as well. The event will be given in a suitable defined form (i.e. Json-format). The HHD tool's event record will be attributed to the rest of the relevant data by the Border Guard Application according to the specific defined configuration. No specific data is stored permanently on-board the HHD tool. There is no need to send any other information concerning i.e. the signal processing, to the iBorderCtrl database.

6.4.2 Technical requirements for HHD tool

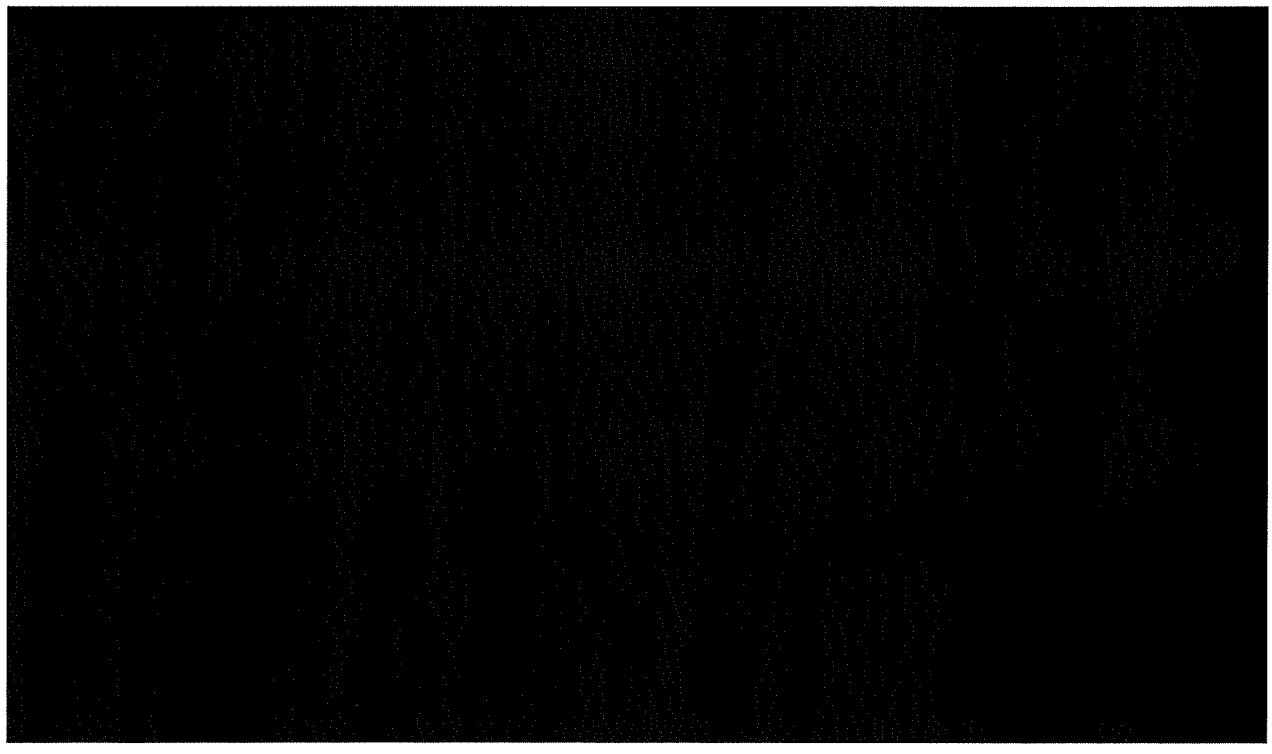
From all the above description so far, it is seen that the HHD tool is different from the patterns that follow the other iBorderCtrl modules i.e. biometrics or document authenticity devices. Unlike the rest of the tools, the HHD tool is solely a data acquisition device that needs to provide the presence detection signal in a format suitable to the iBorderCtrl platform and risk assessment tools. Thus, no comparison with previously stored acquired data or within databases is needed, while the whole unit should enable connectivity with the portable unit and interact with the Border Guards Application.

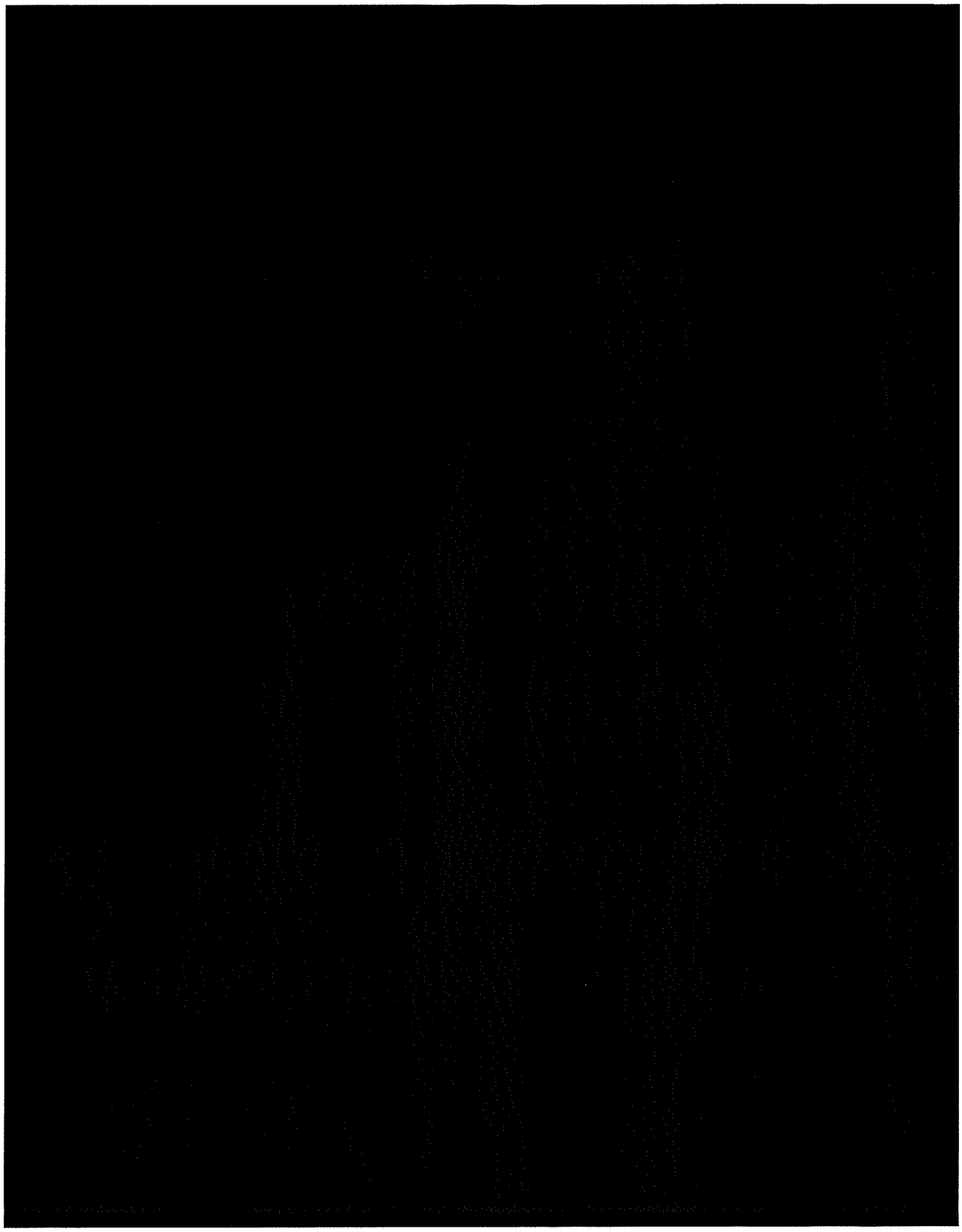
In this sense, and when seen as a sub-system, the HHD tool could also be an independent unit. There are no specific limitations or conditions that affect the iBorderCtrl system or the interaction of the HHD tool with other modules of the iBorderCtrl system.

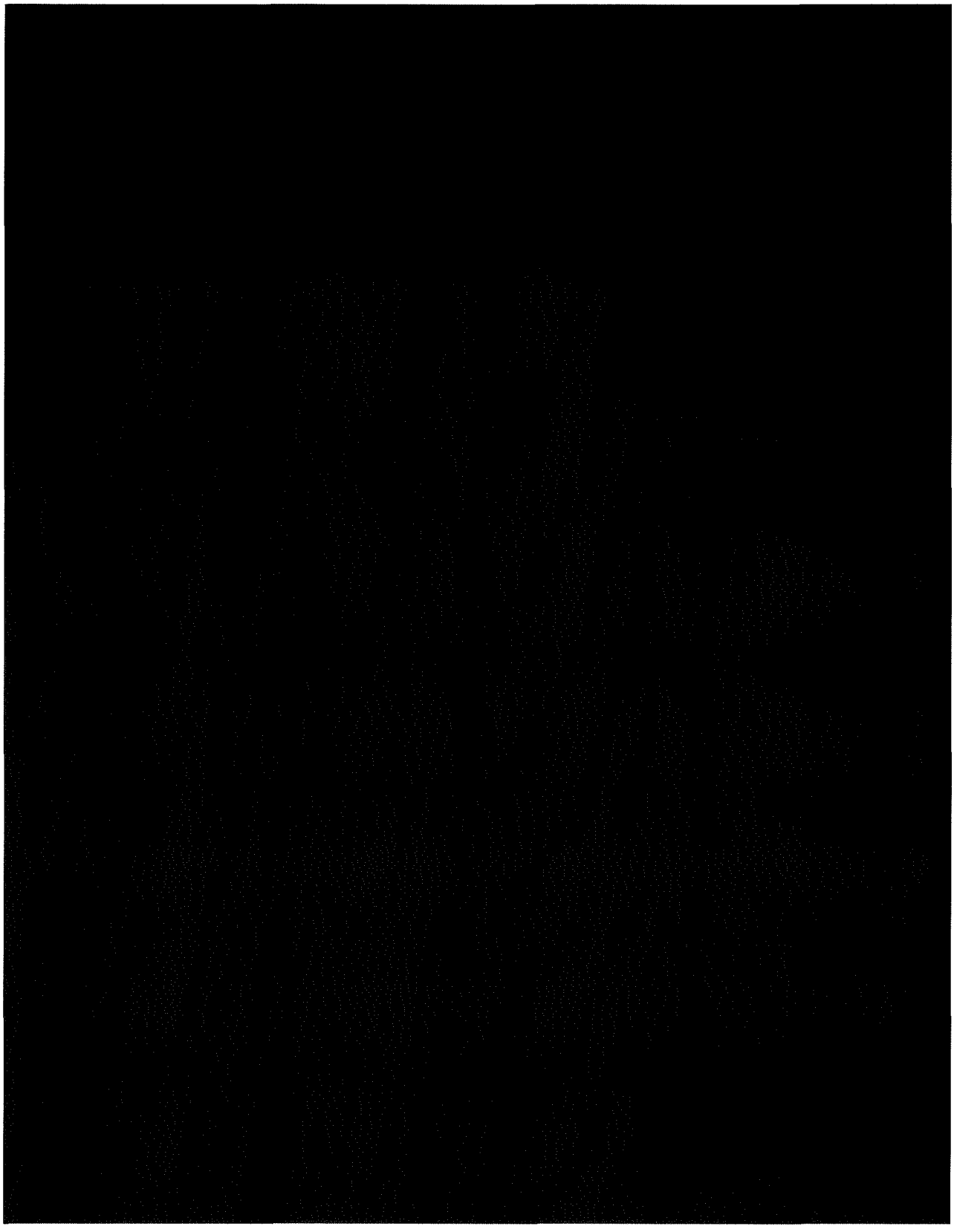
To this respect, the commercially available solutions that are examined for the selection of sensors or even for the selection of more complete systems should address the above dimensions as well, as this will be analysed in the next paragraph.

The key technical challenges that affect the HHD tool and thus further define its specific technical requirements address the following trade-offs:

- The determination of the exact sensing device for each technology may affect the overall performance of the tool along with the portability level. In certain cases, close proximity or direct contact with the subject is needed (geophones sensors). For the EM and acoustic sensors, the range of operation is a trade-off with the emitted / required received power so, depending on the implementation and the performance required, close proximity may be needed as well. These reflect each technology's limitations and thus affect the HHD tool itself, in order to ensure adequate performance.
- Another very important challenge the signal processing algorithms are the main trade-off and those ones that define each technology performance. From the analysis of commercial solutions in the previous sections, it is seen that a variety of signal processing and imaging algorithms are used depending on the technology, performance and usage requirements. However, it should be noted that development of extreme or very sophisticated algorithms for unnecessary imaging features in the framework of iBorderCtrl should rather be avoided; since the main aim is to provide a risk score to be integrated with the relevant scores of the rest of the modules, so to result in a holistic platform for the assistance of the Border Guards' decisions and not to compete with commercial companies.
- The HHD tool as well as the sensors must be able to perform in the harsh conditions that can be found in the Border Crossing Points. This includes resistance against rain, low and high temperatures, dust, etc. The HHD tool equipment will be compliant with the Portable Unit equipment requirements. Concerning each sensor itself, the compliance to the above should be further examined per sensor depending on what is available commercially. However, all sensors will be operating at least to ambient environmental conditions with tamper protection.



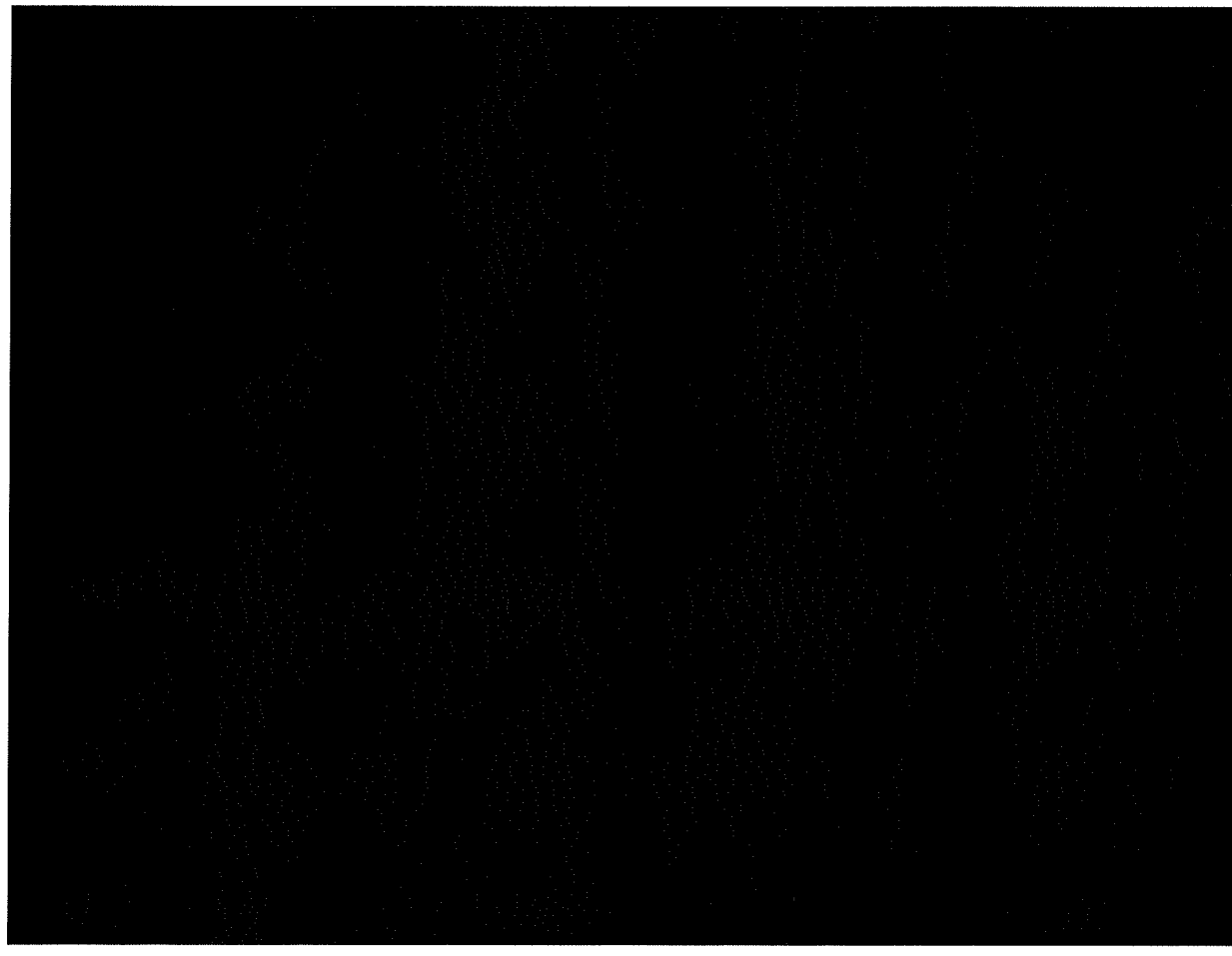




7 Conclusions

The hereby document presents an insightful view on the sensor technologies including biometric, document analysis and hidden people detection tools which might come in handy while implementing iBorderCtrl system components such as ADDS, BIO, FMT, DAAT or HHD. The analysis has been carried out in compliance with the requirements stipulated in WP2, specifically D2.1 and D2.2. The carried out study will constitute a basis for further works performed within WP3 related to the development of iBorderCtrl system components.

The report highlights the importance and impact of spoofing upon daily border control procedures. It has been identified that impersonation is the prevalent and most common method of illegal border crossing attempts. Therefore, iBorderCtrl approach with multimodal biometrics, document authentication, and hidden people detection might provide a system which is suitable, usable and tailored to the actual needs of border guards. In order to mitigate the risk of spoofing, the report pinpoints several effective countermeasures, which have been categorized as software and hardware based.



Appendix A – Counter-spoofing techniques comparison