

A hand is shown from the right side, pointing its index finger towards a glowing network of white nodes and lines. The network is composed of interconnected white dots of varying sizes, with some dots being significantly larger and brighter than others. The lines connecting the dots are thin and white. The background is a dark blue gradient, with the network appearing to recede into the distance. The overall effect is one of digital connectivity and biometric technology.

**MANTRA**  
*Innovation that counts*

# Biometric ecosystem

[www.mantratec.com](http://www.mantratec.com)

## Table of Contents:

■ Abstract .....	3
■ Introduction.....	4
■ Biometric market .....	5
■ Biometric Applications.....	6
■ How Does Biometric Technology Works?.....	7
■ Parameters for the selection of biometrics.....	8
■ Types of Sensing techniques.....	9
■ Multi Fingerprint Scanner.....	9
■ Dual Iris Scanner.....	10
■ Reference.....	13
■ About Mantra Softech.....	13



## I Abstract

With the evolving market needs in the field of biometric technology, researchers are continuously directing their efforts to augment the current biometric recognition techniques. Market is now offering advanced biometric devices which are integrated with more robust, secure, and scalable features such as multimodal approaches, liveness detection, touchless technology thereby overcoming the current security gaps in the biometric scanning technology and ensuring the emerging usage and acceptance rates of biometrics across a wide range of applications and markets. Currently two such biometric scanning techniques offered by Mantra Softech i.e Multi fingerprint scanners and Dual iris scanners are paving the way for more smart, secure and convenient solutions for enrollment of individuals in various identity applications based on biometric technology i.e national identity projects, national population register projects, voter identity projects, border security, criminal identification, and immigration management.

## I Abbreviations

Sr.No	Acronyms	Full forms
1	UNESCO	United Nations Educational, Scientific and Cultural Organization
2	CAGR	Compound Annual Growth Rate
3	BFSI	Banking, Financial services and Insurance
4	AI	Artificial Intelligence
5	AFIS	The Automated Fingerprint Identification System
6	FAR	False Acceptance Rate
7	FRR	False Rejection Rate
8	UID	Unique Identification Authority of India
9	NPR	National Population Register
10	SDK	Software Development Kit
11	WHQL	Windows Hardware Quality Labs testing
12	LED	Light Emitting Diode
13	KYC	Know Your Customer
14	ISO	International Organisation for Standardisation
15	STQC	Standardisation Testing and Quality Certification



## I Introduction

The rising demand for integrated security technologies, personal data protection and access control requirements has resulted in the significant adoption of biometrics system over the years. Information technology, finance, retail, healthcare, e-commerce, and governments are demonstrating the real appetite for the usage of biometrics. Financial institutions like banks around the world are exploring the use of smart cards and biometrics for more accurate verification of their customer and securing online transactions.

A biometric technology identifies the individual based on physiological and behavioural characteristics thus meets more stringent security requirements while relieving users from the burden of remembering passwords or pins. Fingerprints, face, and iris are amongst the most popular physiological characteristics used in commercial biometric systems. Biometrics are being employed in number of diverse applications in the areas of national identity, monitoring time & attendance, immigration management to automate the flow of law abiding travellers and deter illegal migrants, military work and to covert surveillance by automatically identifying suspects entering the crowded security areas like airports.

Currently, around the world, advanced biometric sensing techniques such as fingerprint & Iris are being used for the enrollment & verification of the citizens under various government led initiatives such as national identity project, national population register projects, voter identity projects, border security, criminal identification, and immigration management.

This paper will explain the biometric ecosystem covering the key growth drivers & forecast estimated by research reports, application of biometrics and how it works, parameters for selection of biometrics enrollment system, with special focus on the choice of sensing techniques i.e multi fingerprint & dual Iris scanning technology.



## I Biometric Identification Market

As per a market research report, the Biometric system market size is projected to grow USD 36.6 billion in 2020 to USD 68.6 billion by 2025 at a CAGR of 13.4% during the forecast period. (1)

According to another market research report, Biometric Technology Market size is expected to garner \$10.72 billion by 2022, registering a CAGR of 19.4% during the forecast period of 2020-22 (2)



**Market is estimated to grow at CAGR of 13.4%**

**Figure 1: Biometric market size**

The key factors propelling the growth of the biometric system market are as follows.

- ◆ Growing applications of biometric solutions in the commercial & government sectors and the increasing need for enhanced security systems in organizations.
- ◆ The rise in airport security initiatives after 9/11 tragedy, heightened threat of illegal material smuggling, and extensive use of fake ID for immigration.
- ◆ Growing need for citizen enrollment by governments has increased investment in biometric system globally. In developed countries, advanced biometrics are being used to implement various government projects such as e-passports, citizen enrollment programs such as national ID, e-driving licences, and border control. The fingerprint sensor market is expanding as a result of increased government support for fingerprint sensor adoption, as well as the application of biometrics in the BFSI and telecom sectors for doing KYC of their customers.
- ◆ Evolving multilevel biometric technology, use of biometric technology in cloud computing and blockchain technologies have created growth opportunities for prominent players operating in the global biometric market.
- ◆ The surging adoption of biometric technology in automotive applications and consumer electronic devices for authentication and identification purposes has open the new doors of opportunities.

## I Forecast

- ◆ The market will overall witness a high demand for integrated security technologies, with most growth led by players in manufacturing, healthcare, aviation, government, and law enforcement.
- ◆ Iris recognition system is one of the most appreciated technologies owing to its speed of operation and resistance to false matches compared with other technologies. It is preferred in various countries for security purposes at crucial places, such as airports, government buildings, point of entries and exits in the country, and other applications. The demand for iris recognition systems is expected to increase during the forecast period owing to its higher adoption in multiple end-user verticals.
- ◆ Fingerprint recognition systems have witnessed wide acceptance in various applications owing to novel technology, affordable price, and easy usage. The increasing adaptation of fingerprint recognition biometric system in tablets, mobile devices, POS devices, and cloud computing along with emerging security aspects of fingerprint technology are expected to generate a high demand in the biometric technology market.
- ◆ By deploying biometric authentication and identification, BFSI and Telecom sector aim to boost security and accountability in their infrastructures by doing eKYC of their customer.
- ◆ Multi-factor authentication is expected to be the fastest-growing segment by authentication type, led by the government and defence sectors.
- ◆ Contactless modalities such as face and IRIS recognition will grow faster than contact system due to covid pandemic, although the contact system also plays an important role due to its accuracy and easy enrollment functionality with universal data format for identification and verification through various devices.
- ◆ Growing demand for kiosk and POS devices with biometric fingerprint sensors are also expected to boost the market.
- ◆ The North America biometric system market is projected to reach USD 19.5 bn by 2025 at CAGR of 11.1 %. It is due to increased government investment to install biometric systems.
- ◆ The adoption of cloud-based technology, blockchain technology and AI for biometric devices is expected to boost the requirement for associated software to ensure the compatibility of devices and operating systems for different applications.

## I Application of Biometrics

Biometrics can assist make transactions safer and more feasible for security reasons. It is used for variety of applications and can be divided into three groups.

<p><b>Commercial applications</b></p>	<ul style="list-style-type: none"> <li>● Access control (logical &amp; physical access)</li> <li>● Time &amp; attendance management</li> <li>● eKYC in Financial services &amp; Banks and Telecom sector</li> </ul>
<p><b>Government applications</b></p>	<ul style="list-style-type: none"> <li>● Border Control / Airports</li> <li>● Security and Immigration checks</li> <li>● Food distribution Systems</li> <li>● Healthcare &amp; Social Services</li> <li>● Education sector</li> <li>● Citizen ID</li> </ul>
<p><b>Forensic applications</b></p>	<ul style="list-style-type: none"> <li>● Criminal identification</li> <li>● Surveillance</li> </ul>

## I How does Biometric Technology Works?

There are various types of biometric systems, including facial recognition, hand geometry, iris recognition, retina recognition, and speaker recognition.

**Enrollment, Verification, Identification, and Screening are the processes common to these systems.**



### Enrollment

Enrollment describes the process of registering with a biometric system, which involves creating an account for the first time. It's a one-time process that should take 2 minutes or less.

In the enrollment step, the user needs to prove his or her identity, furnishes the identification document. The biometric characteristics of the concerned user are linked to the identity specified in the identification document. This ensures that the reference template is linked to the right identity. This is a key step which determines the integrity of the system.

After the enrollment process the user provides any or the required biometric samples (like Fingerprint, Iris Pattern or Hand Geometry) to an acquisition device, usually a biometric sensor. Here the system acts operates in the data acquisition mode, where the device or scanner is used to populate the database.

The acquired data is encrypted using any secure algorithm and stored in the central/remote database. The storage can also be made in the memory chips or cards. The user may need to enroll and present the samples multiple times as small changes in positioning, distance, pressure, environment, and other factors influence the generation of a template, and it is expected to be unique.

Therefore, a person may need to present biometric data several times in order to enroll. The reference template may then represent an amalgam of the captured data, or several enrollment templates may be stored. In addition, because biometric features can change over time, people may have to reenroll to update their reference template.



### Verification

The verification step (one to one comparison for subject verification) to establish an individual identity) objective is to confirm that a person is in fact who he or she claims to be. Here the real time input is compared with the stored template to determine whether or not there is a match. Verification is always considered to be "one-to-one" matching. Out of the millions of reference templates, only one needs to be compared to the sample template. The output of the verification systems is a match /no match decision in less than a second. In case of using multimodal or liveness detection priorities are set and also the system acts as a toll gate.



### Identification

The identification systems are considered to perform "one-to-many" matching, where the sample template is compared against the stored reference templates of all individuals enrolled in the system. There are two types of identification systems – Positive and Negative. Positive identification systems: Determine whether a user seeking access can be identified as having been enrolled in the system. Negative identification systems: Ensures that a users' biometric information is not present in a database. For example, a negative identification system may be designed to identify people on a watch list.



### Screening

It is a step where the input templates are collected from many users and the process of comparing is done with all the Enrolled reference templates. It is considered to be "many to many" matching. The outcome of this step is a decision where it notifies X people out of the Nnumbers are identified.

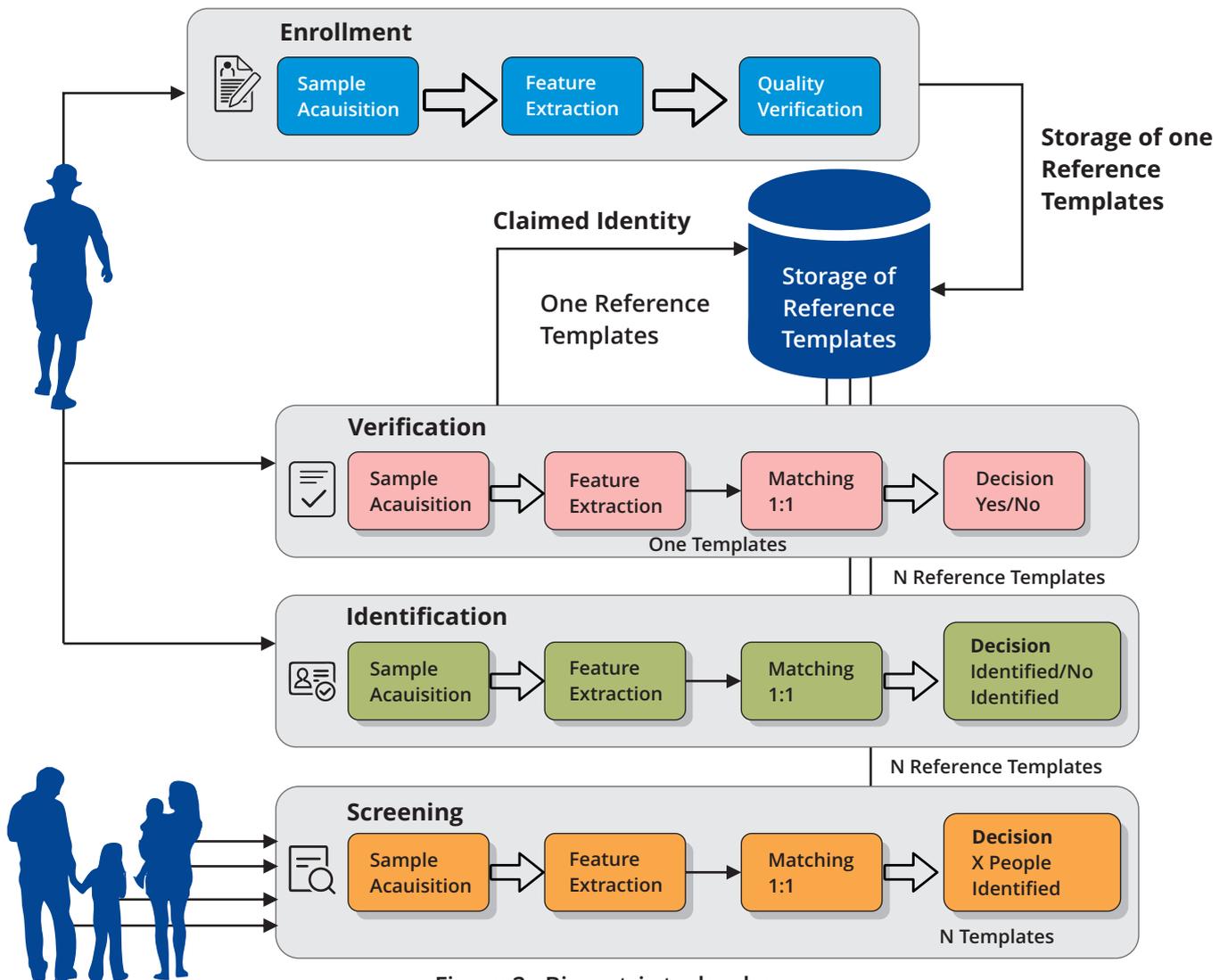


Figure 2 : Biometric technology process

## I Parameters for the Selection of Biometrics

Researchers recognised various crucial factors that are essential characteristic needs of any biometric attributes. These features are sometimes referred to as the "seven pillars of biometrics."

 <b>Universality</b>	Every individual in the target population should possess the trait.
 <b>Performance</b>	High recognition accuracy such as FAR & FRR and speed should be achievable with limited resources in a variety of operational and environmental conditions.
 <b>Acceptability</b>	The biometric identifier should have a wide public acceptance and the device used for measurement should be harmless.
 <b>Circumvention</b>	Spoofing of the characteristic using fraudulent methods should be difficult.
 <b>Collectability</b>	The trait should be easily obtainable (or measurable)
 <b>Permanence</b>	The biometric trait should be constant for certain period of time
 <b>Uniqueness</b>	Each person should have the feature but distinct from others.

The gradual shift in the biometric landscape is presenting challenges for the researchers to introduce advanced features in the new generation devices. In addition to the above basic attributes, there has been huge demand for features which can overcome current gaps. Many enrollment devices till today doesn't satisfy the end user requirements

Some of these key challenges are as follows-

- ◆ Absence of Liveness detection feature.
- ◆ Credibility concerns related to IP65 enclosures standards and ISO
- ◆ Limited usage of applications with Operating System i.e windows linux android and IOS.
- ◆ Compromised efficacy in harsh environment such as under direct sunlight, shade or moist environment.
- ◆ Ability of the device to work under poor quality of biometric physiological characteristics.
- ◆ Lack of robustness, flexibility and scalability.
- ◆ Highly complex in large scale biometric enrollment and verification.
- ◆ High cost of implementation for larger audiences.
- ◆ Majority of players in industry lack experience of citizen identification application.
- ◆ Lack of Infrastructure and trained staff to perform the identification and verification process.

## I Sensing Techniques for Enrollment & Verification

The most well-known types of biometric securities are fingerprint scanning and iris scanning, both are often utilised to carry out the enrollment and verification process of the citizens.



### Fingerprint scanners

The earliest and most well-known biometric identification method is fingerprint recognition. It's a digital, automated version of the old ink-and-paper method used by law enforcement authorities for identification. It is based on the analysis of an individual's fingerprint to recognise it. Fingerprints are unique and immutable to each individual, and their fundamental properties do not alter over time. Even identical twins' fingerprints are different. Furthermore, the fingerprints on the same individual's two fingers differ. A fingerprint consists of ridges and furrows. The two fundamental principles immutability (ridge patterns never change during the life time) and uniqueness (distinct ridge patterns on different fingers of the same individual) are used in identification of individual's fingerprint.



### Single Fingerprint scanner

A single fingerprint reader have the ability to capture only one finger print for identification and verification.



### Multi Fingerprint scanner

Multi fingerprint scanners are gaining lot of attention as these devices have wide scanning area to capture all ten fingerprints (four finger-slaps and thumbs of both the hand) hence; allowing the user to scan both hands rolled and flats fingerprint of an individual. Moreover, accuracy of single finger scanning may be impacted by damaged or dirty finger so it's a good idea to use multi fingerscanning with ISO format image capturing feature which not only reduces the FRR and FAR issues but also fetches higher degree of reliability and durability.

Now a days, many local/government organizations are efficiently utilising the multi fingerprint scanners for multiple commercial, civil and government applications.



# MORPHS

## Multi Fingerprint Scanner



10 Finger Capture



FBI Appendix F-Compliance



IP54 Surface



Scratch-Free Surface



ANSI/NIST Standards



LED Indicators

### I MORPHS – Multi Fingerprint scanner

Mantra Softech has always been dedicated to delivering cutting-edge devices by thoroughly understanding current market demands and relying on industry best practices.

The Multi Fingerprint scanner has been meticulously designed to provide customers with an outstanding experience while taking into account both basic and advanced requirements thereby mitigating the challenges faced by current set of available enrollment devices.

MORPHS is a unique & portable ten-print fingerprint capture (four finger-slaps & thumbs of both the hands) device which is ideal for delivering fast, accurate and reliable fingerprint capture results for biometric verification, identification and enrollment applications.

MORPHS is widely used for enrolling citizens by local or central government organizations, UID-Aadhaar in India, NPR, National ID projects, World Bank and UNESCO schemes.

Additionally, an ergonomic design combined with an easy-to-integrate SDK architecture makes MORPHS the perfect choice for system integrators and solution providers.

### I Key Features of MORPHS



Single flat finger image capture



Device Driver - WHQL certified Device Driver



Better User Interface by LED Indicators.



Image Quality - FBI Appendix F-Compliance



Ingress Protection rating Ip65



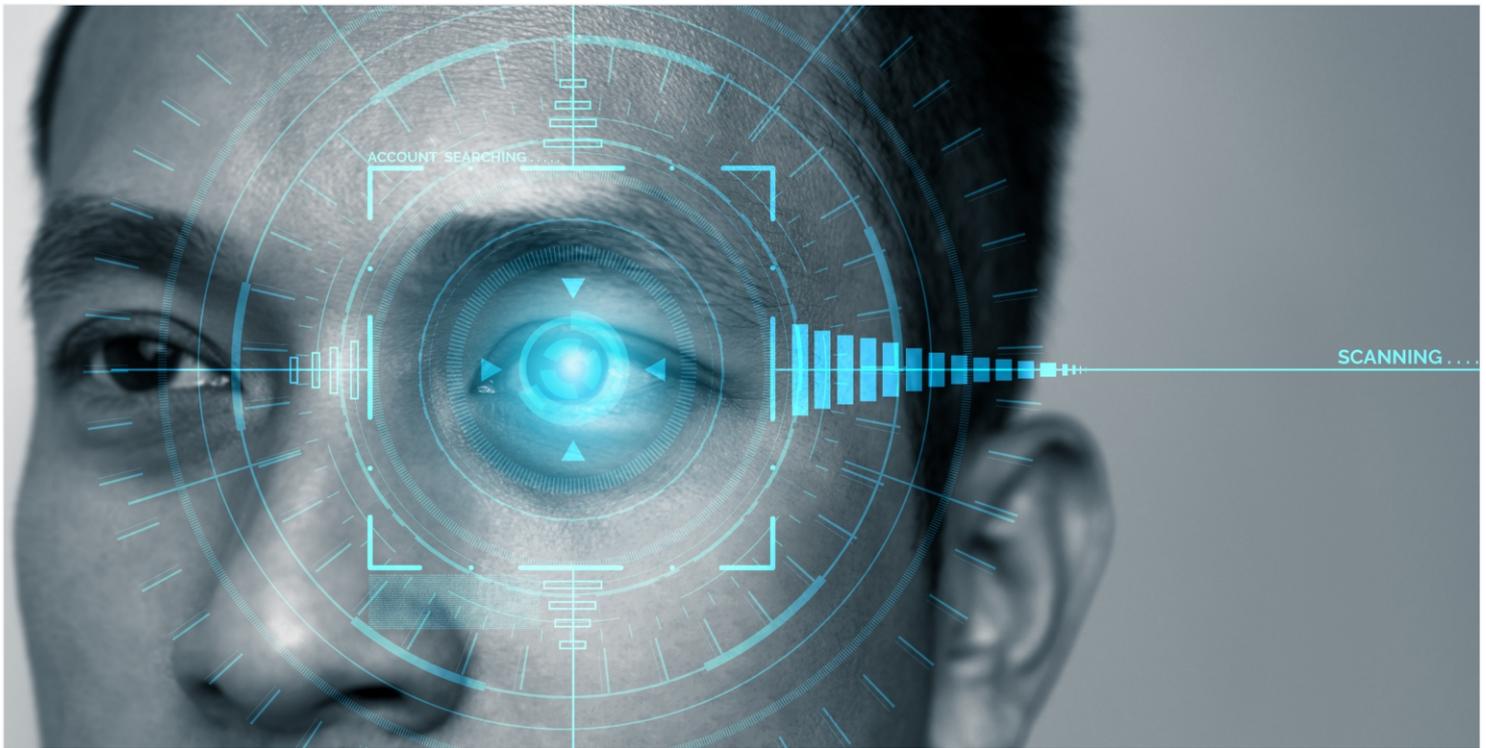
Sensor type- Scratch free sensor surface



Interface- USB 2.0, USB-IF certified



Capturing Format Registers four finger-slaps & two thumbs of both the hands.



## I Defining IRIS scanners

The second biometric sensing technique extensively popular for enrollment & verification of citizens are IRIS scanners.

Iris scanning is a non-invasive process that identifies or authenticates an individual by analysing the unique patterns in the iris portion of the eye. The iris is the coloured part of the middle coat of the eye behind the cornea and surrounds the pupil. It is unique to an individual and remains stable with age as per the research studies. The iris is guarded by cornea so it remains protected from any damage hence becomes quite suitable for biometric identification and authentication process.



### Single Scanner

The patterns on the iris of an individual both eyes are fairly distinct from one another and even genetically identical twins have different iris patterns. This touchless scanning technique relies on only one iris for the purpose for enrollment.

In this technique, obtaining a decent quality picture of an iris in a less confined setting which has a diameter of roughly 1 cm, is extremely challenging, especially from a wider distance. The quality of the iris picture is also affected by several types of noise making it less preferred choice of biometric recognition.



### Dual Iris scanning

This scanning technique uses both the left and right iris of the individual for performing the recognition. This latest scanning is based on newer infrared techniques with the goal of identifying the iris from a distance or even while the person is walking. To improve accuracy, these techniques rely on a dual iris approach whereas the classical Infrared methods perform well only in constrained environments and when the distance between the user and the capturing device is small. The dual iris approach outperforms the single iris approach, especially if the number of enrolled images/eye is small.

Dual Iris scanners have significantly higher accuracy in both verification and identification scenarios, making them an excellent choice for practical security.

# MATISX

## DUAL IRIS SCANNER

Mantra Softech is a Global Hi-Tech Manufacturer of Biometric Products & Solutions. We Offer a Wide Range of Products in Biometric and RFID Industry.



### I MATISX –Dual Iris Scanner

With an aim to offer the highly innovative future ready superior products in the field of biometrics, Mantra Softech has designed MATISX, an advanced dual iris scanner that simultaneously captures both the iris of an individual with greater precision and accuracy.

Designed with an advanced biometric technology, MATISX is the next-generation dual iris scanner device compliant with ANSI NIST and ISO image interchange format.

The adjustable interpupillary distance feature makes the device well-suited for IRIS based biometric identification & enrollment project requirements.

### I Key Features of MATISX

- 

Touchless/Contactless – MATISX provides a touchless feature which makes it hygienic to use and less intrusive to the end user.
- 

IP65 certified - it is enclosed in a sturdy casing that provides protection against dust and water.
- 

Easy to use - The dual iris sensor presents multiple compelling functionalities such as auto capture feature for quick & effortless dual iris recognition.
- 

Flexible & Scalable - These infrared scanners are quite flexible as it has adjustable interpupillary distance range further it can be used at night or in low light and immune to ambient light conditions, making it extremely scalable for deployment.
- 

Cost effective - MATISX is cost effective as it explores the proven technology which is easy to understand hence reduces the cost of testing.
- 

User friendly - The innovative dual iris scanner MATISX offers ease of convenience, high reliability and long-lasting durability.
- 

High efficacy – MATISX is unaffected by eyeglasses, contact lenses, caps, or masks, and it works well for children and blind persons with iris.
- 

Liveness detection - The iris scanner technology detects the movement of the iris and validates the genuine presence of individual thus lowering the possibility of spoof attempt.

## I Conclusion

A proven robust and versatile enrollment solution is highly imperative for big scale government, social welfare programs and commercial initiatives. Multi Fingerprint scanner and Dual Iris scanners are two such enrollment devices that have gained lot of attention in the market due to its exemplary features and increased usage in various government led projects around the world related to Unique identification, facilitating regular and safe cross-border mobility and managing migrants thus contributing towards increasing security for all.

Biometrics systems are used all over the globe and have penetrated numerous markets, yet biometric technologies are continuously growing and gaining traction. Additionally, efforts are being undertaken to standardise common software interfaces in order to facilitate the exchange of biometric templates as well as the effective comparison and assessment of different biometric technologies such as MOSIP developed by IIT Bangalore.

The security of the user's template remains a key problem for biometric systems. Because the templates reflect the user's personal characters, they offer a risk of violating one's privacy if they are not securely kept. The fact that the template is stored in a centralised database makes it vulnerable to assault and compromise. Smart cards are one of the options being considered for safe storage, since they will improve individual privacy and boost security from assaults by allowing individuals to manage their own templates. Another way is cryptographic biometric devices which can be used to personalise a biometric to encode a PIN, a password, or an alphanumeric string for a variety of applications such as bank ATMs, building access, and computer terminal access. Furthermore, the database only needs to keep the biometrically encrypted PIN or password, not the entire biometric sample.

In the next generation of identity and security solutions, biometrics has a bright future. It is now the ideal moment for businesses to improve their biometric skills and invest in biometrics-related technology in order to meet industry needs.

## I References

- ◆ Biometrics System market - Global Forecast to 2025 by marketsandmarkets1.
- ◆ Biometric Technology Market- Global Opportunity Analysis and Industry Forecast, 2015 – 2022 by Allied Market Research2.
- ◆ Next generation biometrics market - growth, trends, covid-19 impact, and forecasts, 2021 – 2026 by Mordorintelligence.
- ◆ Fingerprint Sensor Market - Global Opportunity Analysis and Industry Forecast, 2020–2027 by Allied Market Research.
- ◆ Recent advances in emerging biometrics (2013) by C. Sesha Ratnam, C.Raja, G.Ramesh, N.V.Vinodkumar & N.Jyothsna.
- ◆ A Comprehensive Survey on Various Biometric Systems (2018) by T.Sabhanayagam, Dr. V. Prasanna Venkatesan and Dr. K. Senthamaraiannan.

## I About Mantra Softech

Mantra Softech is a leading STQC certified manufacturer of the key Biometric products and has been active since 2006. The company's Multi Fingerprint Scanner & Dual Iris Scanner has been currently being used in various government led projects and commercial initiatives and is the most preferred choice among other scanners in the market.

Mantra Softech is the pioneer of Aadhaar, enabling biometric devices which are currently used by the Indian government for the social welfare scheme, and also by telecom and banking sector for KYC purposes. The manufacturing units are equipped with cutting-edge technology, intense automation and zero chance of human error.

Mantra Softech is one of the few players in the industry to have state-of-art R&D facilities in Ahmedabad, India approved by Ministry of Electronics and Information technology of India with an aim to improve product functionality and develop new products which are future proof. As for quality standards, Mantra is committed to the core values of integrity, ethical practices and responsibility towards customers and the environment. Brilliant quality and design achieved by the vision of our leaders, has led to the rapid growth of Mantra as a global brand and Mantra has now become a powerhouse of biometric innovations in just a few years even though it is just a beginning.

Mantra's focus is to provide innovative products and solutions with a set of innovation. Mantra emphasizes to promote intellectual qualities in an individual and amongst the team to provide the best solutions before various clients in a cost-effective manner.

For more information, visit [www.mantratec.com](http://www.mantratec.com)

# MANTRA

[www.mantratec.com](http://www.mantratec.com)



+91-79-49068001



[sales@mantratec.com](mailto:sales@mantratec.com)