ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 11, November 2025

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

App for Protecting the Future

S. Manoj Kumar, Namitha Velpula

UG Student, Dept. of ECE, Jain University, Bangalore, Karnataka, India

UG Student, Dept. of ECE, Jain University, Bangalore, Karnataka, India

ABSTRACT: The "App for Protecting Future" presents an application that assures safe digital experiences through the integration of age recognition, face detection, and privacy- oriented content control. A feature-based facial algorithm, GAN-based age progression, and biometric authentication involve verification of the identity of a user, determination of age suitability, and prohibition of access to unsuitable content. The architecture of the app will include modules on filtering of content based on age, management of cookies, restriction of content, and storage of documents in a secure way with encryption and controls for access rights. Mobile hardware, image-processing libraries, and privacy-compliant APIs support the proposed architecture in creating a personalized and secure environment that protects children and users from harmful digital exposure while securing sensitive information with robust security and privacy mechanisms.

KEYWORDS: Age recognition Facial detection, Biometric authentication, Generative adversarial networks (GANs), Content filtering, Privacy protection, and Secure data storage

I. INTRODUCTION

Background

Age recognition, face detection, and content release are interconnected technologies with various applications across industries such as security, marketing, entertainment, and healthcare.

Age recognition technology involves identifying and estimating the age of individuals from images or video footage. It typically utilizes machine learning algorithms trained on large datasets of facial images. Age recognition has applications in age-restricted content filtering, targeted advertising, and demographic analysis.

Face detection algorithms detect facial features such as eyes, nose, and mouth, and then use pattern recognition techniques to determine whether a region of the image contains a face. Face detection is used in various applications, including facial recognition for security systems, automatic tagging in photo management software, and emotion analysis in market research.

Content release refers to the process of distributing digital content, such as movies, music, or software, to the intended audience. Age recognition and face detection technologies play a role in content release by enabling content providers to enforce age restrictions and customize content based on the viewer's demographics. For example, streaming platforms may use age recognition to restrict access to mature content for underage viewers, or they may use facial recognition to personalize recommendations based on the viewer's age and preferences

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

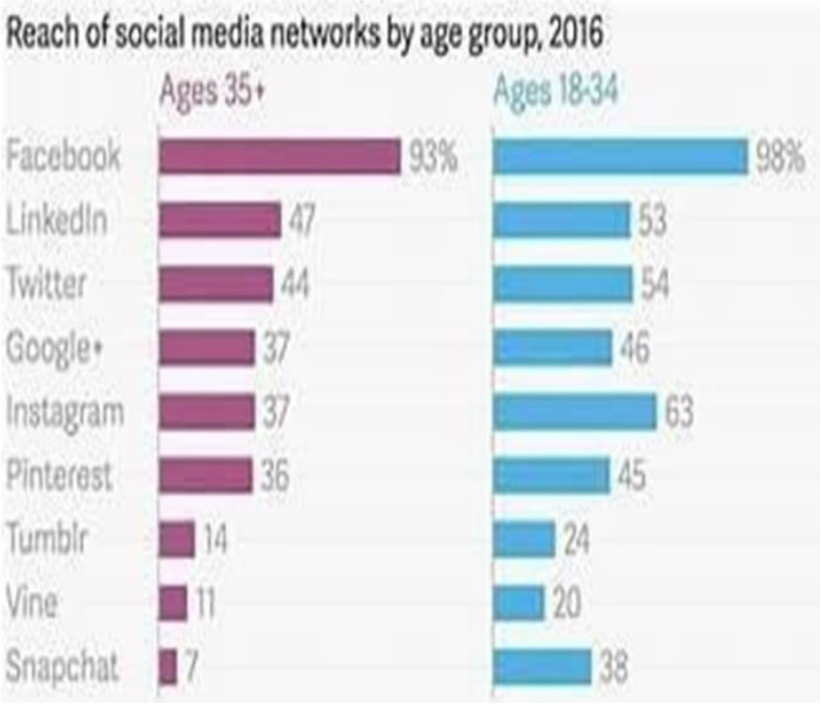

Fig.1: Reach of social media networks by age group, 2016

II. LITERATURE SURVEY

S. No	Year of Publication	Authors	Title of the Paper	Published Journal Name	Problem Addressed	Solution Identified for problem
1	2024	Abraham Woubie , Enoch Solomon , Joseph Attieh	Maintaining Privacy in Face Recognition Using Federated Learning Method	**IEEE**	potential privacy concerns	application of federated learning
2	2024	Dawson, Juehee	Privacy-Enhanced Parenting Mediation System "ProKids" Providing Age-Appropriate Content with X.509 Certificate Age Rating	University of Ottawa	Children's online security and privacy	Parenting mediation tool
3	2024	Sebastian Zimmeck , Eliza Kuller (Wesleyan University), Chunyue Ma (Wesleyan University)	Generalizable Active Privacy Choice	Wesleyan University	Privacy preference signals	Global Privacy Control
4	2024	Bhadkare, Bhavna; Jotwani, Varsha	Enhancing Face Recognition Accuracy On Low-Resolution Databases Using Interpolation Techniques And Feature Extraction Techniques.	Journal of Advanced Zoology, 2024, Vol 45, Issue 3, p46	impact of image resolution on the performance of face recognition systems	Propose methods to enhance recognition accuracy on low-resolution face databases..
5	2024	Zimo Liao , Zhicheng Luo , Qianyi Huang	Gesture Recognition Using Visible Light on Mobile Devices	IEEE	cameras and acoustic signals	in-air gesture recognition , mmWave radar and depth camera.
6	2022	Yonder Consulting	Children's Online User Ages	ofCom	Misuse of online Law	online safety regulator.
7	2023	**Gagandeep Kaur , Kunjal Lalit Pise , Latika Pinjarkar**	in-air gesture recognition	2nd Computing Congress 2023	cybersecurity concerns posed by the growing usage of social media	preventive measures such as privacy enhancements, user training, sophisticated email filtering
8	2022	Janis von bleichert	Reject cookies	Experete	Impact on website's features	General data protection regulation
9	2024	Le Yang, Miao Tian, Duan Xin, Qishuo Cheng, Jiajian Zheng	AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning	Cornell university	existing challenges in machine learning related to privacy and personal data protection	machine learning's differential privacy protection algorithm

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROBLEM FORMULATION AND PROPOSED WORK

Table 2: Problem and Proposed algorithm

Problem	Proposed algorithm
Variability in Facial Appearance	Feature-Based Algorithms
Age Progression	Generative Adversarial Networkes
User Verification	Biometric Authentication

Problem Statement

Variability in Facial Appearance: Facial appearance can vary significantly due to factors like pose, lighting conditions, expressions, and occlusions. These variations make it difficult to accurately match faces across different instances.

Age Progression/Regression: Facial appearance changes over time due to aging, making it difficult to accurately estimate a person's age based on their current facial features. Age progression techniques attempt to simulate the effects of aging, but the accuracy of these methods can vary.

User Verification : Ensuring that the app is used by the appropriate age group is challenging . Implementing robust age verification mechanisms can be complex.

Proposed Algorithms

Feature-Based Algorithms: These algorithms identify specific facial features such as eyes, nose, mouth, and their spatial relationships. They then use these features to create a unique facial signature or template for each individual. Different variations of feature-based algorithms include:

Eigenfaces: This method uses principal component analysis (PCA) to represent faces as a linear combination of basis vectors (eigenfaces). It's effective but sensitive to variations in lighting and facial expressions.

Local Binary Patterns (LBP): LBP focuses on texture patterns in facial images, which makes it robust to variations in lighting and facial expressions.

Generative Adversarial Networks (GANs): GANs have shown significant promise in generating realistic images and have been applied to age progression tasks. In this context, a GAN consists of two neural networks: a generator and a discriminator. The generator learns to generate realistic images of a person at different ages, while the discriminator tries to distinguish between real and generated images. Through adversarial training, the generator improves its ability to produce convincing age- progressed images.

Biometric Authentication: This involves verifying the user's identity based on unique biological characteristics such as fingerprints, facial features, iris patterns, or voiceprints. Algorithms such as fingerprint matching, facial recognition, or iris recognition are used for this purpose.

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. IMPLEMENTATION

Hardware Requirements

1. **Mobile Devices**:

1. Smartphones or tablets with adequate processing power and storage capacity.
2. High-quality cameras capable of capturing clear images or videos.
3. Preferably equipped with biometric sensors such as fingerprint scanners or facial recognition cameras for enhanced security.

2. Sensors:

1. Accelerometer and gyroscope for motion detection and orientation sensing.
2. Proximity sensor for detecting device proximity to the user.
3. Light sensor for adjusting screen brightness based on ambient light conditions.

Hardware Requirements

Operating System:

- Compatibility with major mobile operating systems such as Android and iOS.
- Support for the latest versions of the operating systems to ensure compatibility with the latest features and security updates.

Programming Languages:

- Java or Kotlin for Android development.
- Swift for iOS development.
- Python or other languages for backend development if required.

Privacy Controls and Security Features:

- Implementation of secure authentication mechanisms (e.g., biometric authentication, PIN, password).
- Encryption techniques to protect sensitive user data and communications.
- Compliance with privacy regulations (e.g., GDPR, CCPA) and best practices for data handling and storage.

Content Age Recognition Libraries or APIs:

- Integration with third-party libraries or APIs for age estimation and content classification.
- Open-source or commercial libraries for image and video processing, facial recognition, and age detection.

Overall System Architecture

- The system architecture will utilize advanced algorithms and data analysis to accurately determine the age of the user and control the access to sensitive material.
- The proposed architecture consists of multiple components, including an age verification module, content classification engine, and access control mechanism. These components work together to analyze and categorize content based on age suitability, providing users with a secure and personalized experience.

Flow Diagram of algorithms:

1. Age-Based Content Filtering Algorithm :

- Input: User's age, Content to be displayed
- Output: Filtered content suitable for the user's age Steps:

1. Determine the user's age either through user input or through the device settings.
2. Maintain a database or categorization of content with age appropriateness ratings.
3. Compare the user's age with the age appropriateness ratings of the content.
4. Allow access to content that matches or is below the user's age.
5. Block access to content that exceeds the user's age, optionally with a parental override option.

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

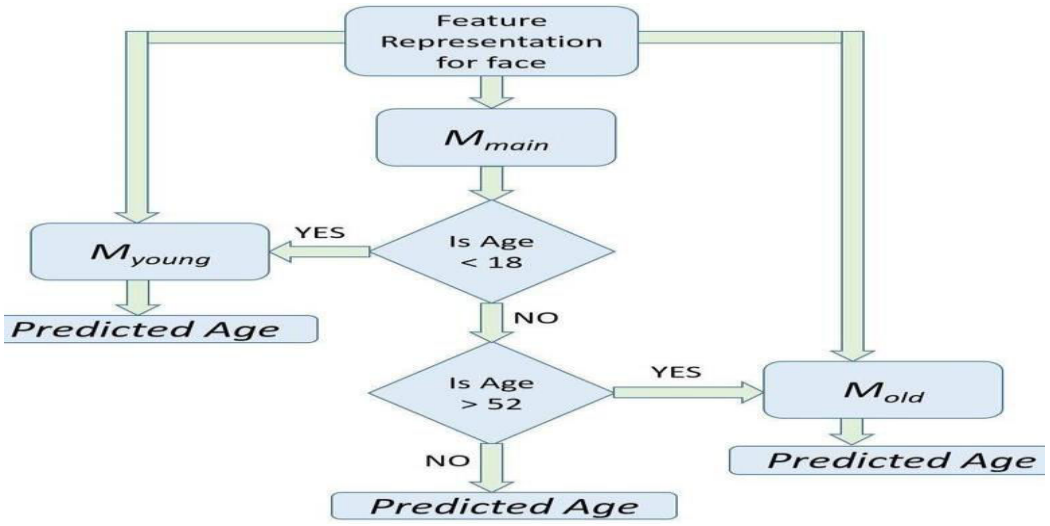

Fig 2: Flow diagram of Age-Based Content Filtering

2. Cookie Management Algorithm:
-Input: Website cookies
-Output: Filtered cookies based on user preferences
Steps:
1. Identify and categorize cookies based on their purpose (e.g., tracking, authentication, preferences).
2. Allow the user to set preferences for cookie types they want to allow or block.
3. Implement a filtering mechanism to block unwanted cookies based on user preferences.
4. Regularly update the filtering mechanism based on user feedback and changes in cookie policies.

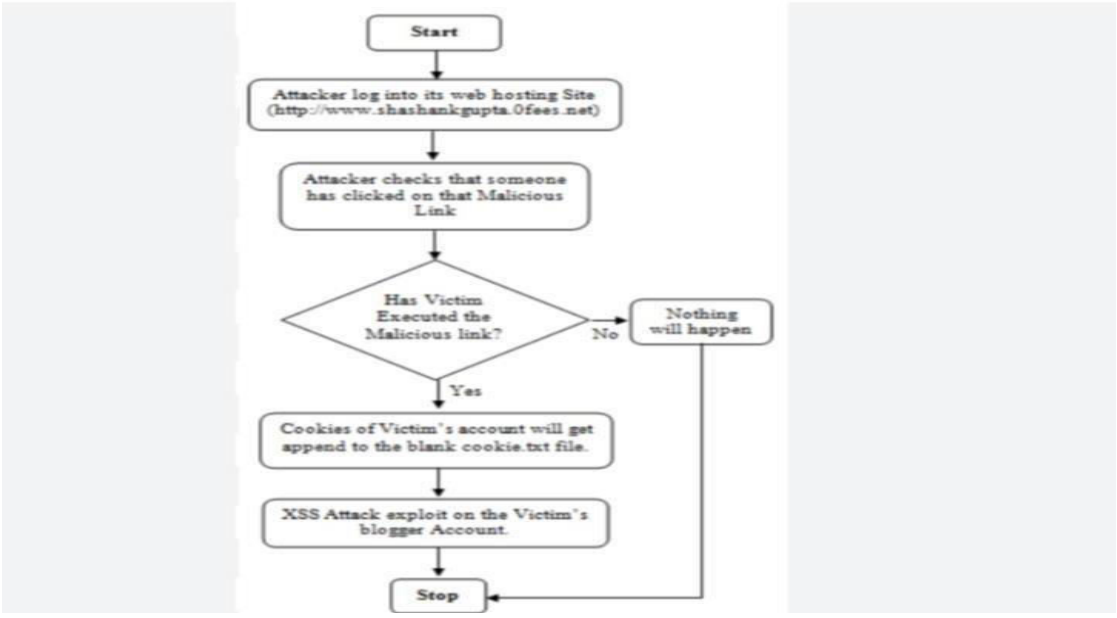

Fig 3: Flow diagram of Cookie Management Algorithm

3. Content Restriction Algorithm:
- Input: Content to be filtered, User's content preferences
- Output: Filtered content based on user preferences

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Steps:

1. Maintain a database of keywords, URLs, or content categories considered inappropriate or unwanted.
2. Allow the user to set preferences for content filtering based on keywords, categories, or specific websites.
3. Implement a filtering mechanism to scan and block content that matches the criteria set by the user.
4. Provide options for the user to customize the level of strictness in content filtering.

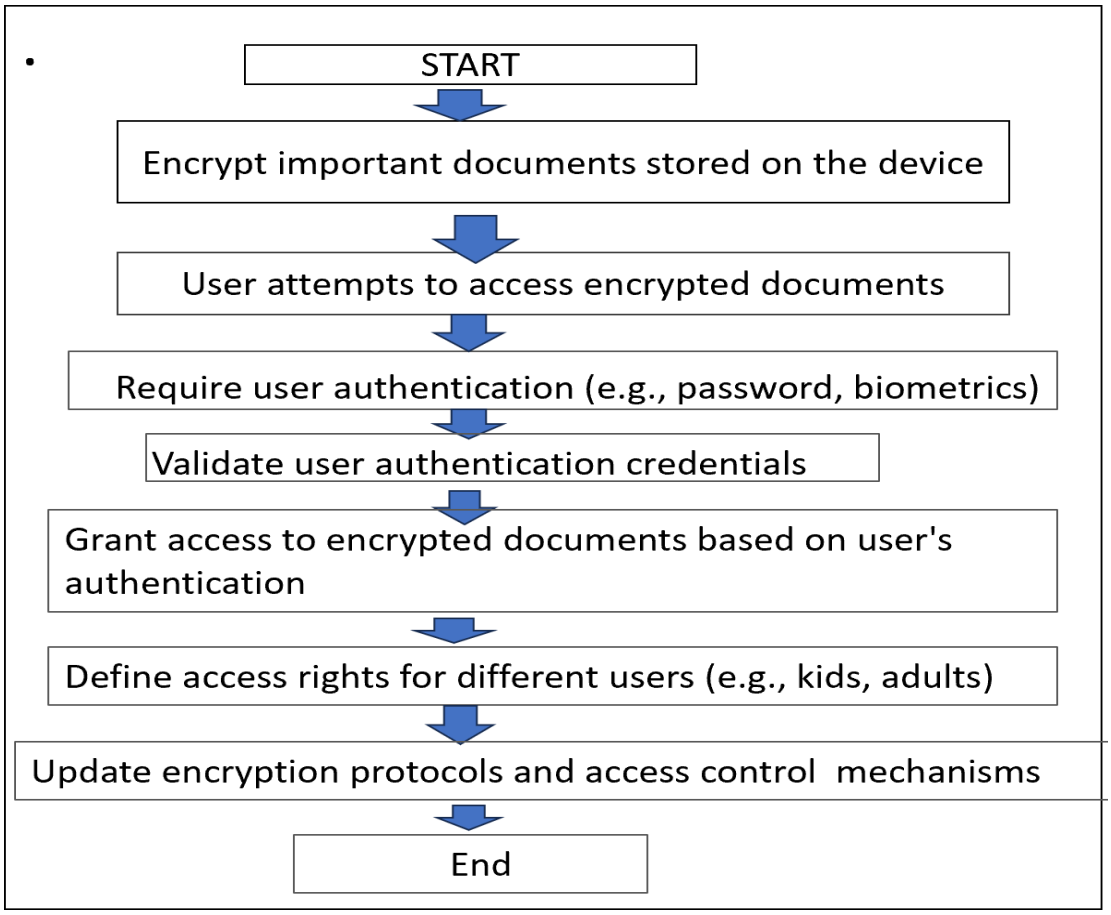

Fig 4 : Flow diagram of Content Restriction Algorithm

4. Document Safeguarding Algorithm :

- Input: Important documents, User's access rights
- Output: Secure storage of important documents

Steps:

1. Implement encryption mechanisms to encrypt important documents stored on the device.
2. Require user authentication (e.g., password, biometrics) to access encrypted documents.
3. Define access rights for different users (e.g., kids, adults) based on their authentication credentials.
4. Regularly update encryption protocols and access control mechanisms to ensure robust security.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

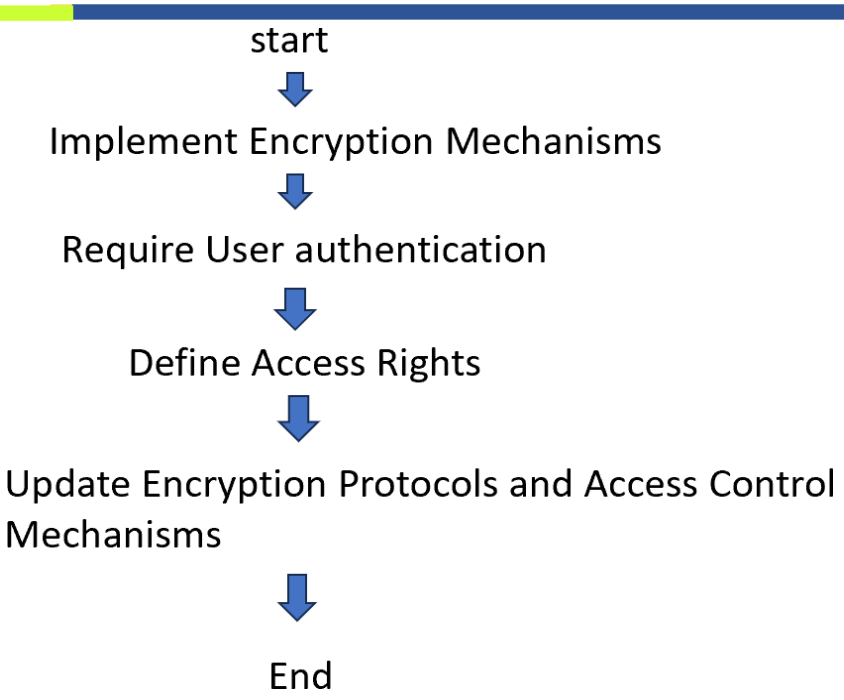

Fig 5: flow diagram of Document Safeguarding Algorithm

V. CONCLUSION

The App for Protecting the Future *represents a proactive step toward leveraging digital innovation for societal well-being, environmental responsibility, and long-term sustainability. By integrating advanced technologies such as artificial intelligence, secure cloud architecture, real-time analytics, and user-centric design, the application empowers individuals and communities to make informed decisions and take meaningful action.*

This initiative demonstrates that technology can go beyond convenience—it can educate, protect, and inspire change. Whether applied to environmental conservation, safety, resource management, or community engagement, the app serves as a bridge between current needs and future resilience. Its scalability, accessibility, and adaptability make it a powerful platform capable of evolving with the challenges and demands of tomorrow.

REFERENCES

1. Maintaining Privacy in Face Recognition Using Federated Learning Method, Abraham Woubie , Enoch Solomon , Joseph Attieh,2024.
2. Privacy-Enhanced Parenting Mediation System "ProKids" Providing Age- Appropriate Content with X.509 Certificate Age Rating, Dawson, Juehee,2024.
3. Generalizable Active Privacy Choice, Sebastian Zimmeck , Eliza Kuller (Wesleyan University), Chunyue Ma (Wesleyan University),2024.
4. Enhancing Face Recognition Accuracy On Low-Resolution Databases Using Interpolation Techniques And Feature Extraction Techniques. Bhadkare, Bhavna; Jotwani, Varsha,2024.
5. Gesture Recognition Using Visible Light on Mobile Devices, Zimo Liao , Zhicheng Luo , Qianyi Huang,2024.
6. Children's Online User Ages , Yonder Consulting,2022
7. In-air gesture recognition , Gagandeep Kaur , Kunjal Lalit Pise , Latika Pinjarkar , 2023.
8. Reject cookies , Janis von bleichert, 2022
9. AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning, Le Yang, Miao Tian, Duan Xin, Qishuo Cheng, Jiajian Zheng,2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com