INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

A PATTERN MATCHING USING POPULAR COMPUTER-BASED BIOMETRIC METHODOLOGIES

Roja D[1], Lavanya Dalavai[2], Ahamad Sharif Sk[3], Venkateswarlu Tata[4], M Venkateswara Rao[5]

[1,2]Assistant Professor, Dept. of CSE-Data Science, Chalapathi Institute of Technology, Guntur, AP, India

[3]Assistant Professor, Dept. of CSE, KHIT, Chowdavaram, Guntur, AP, India

[4]Assistant Professor, Dept. of CSE, Guntur Engineering College, Yanamadala, Guntur, AP, India

[5]Professor, Dept. of CSE, NRI Institute of Technology, Pothavarappadu, Vijayawada, AP, India

ABSTRACT

This present century is full of inventions and discovery, which lead to the invention of many sophisticated things. The more the things are the more the security is needed. This has lead to the invention of many security items. The information age is quickly revolutionizing the way transactions are completed. Every day actions are increasingly being handled electronically, Instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand fast and accurate user identification and authentication. Biometric technology is a way to achieve fast, user-friendly authentication with a high level of accuracy.

While the word “pattern matching using biometrics” sounds very new and “high-tech” in technical terms, It is the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for the purposes of recognizing an individual. This report will highlight some of the popular methods, multimodal biometrics, some of the benefits of using this system for authentication, performance metrics and emerging applications in day to day life. It is evident that our identity is frequently required; for the time being we use a wide assortment of methods to verify our identity: usernames, passwords, signatures, keys, cards etc. Biometrics allow us to authenticate ourselves with things that we carry with us wherever we may go, such as our hands, eyes, voices, faces, fingerprints etc. In addition to the convenience, this can be much more effective; a key or card, for example, can fall into someone else's hands. The promise of ease and increased security are perhaps its most appealing features.

Biometrics is seen by many as a solution to a lot of the user identification and security problems in today’s networks. Password abuse and misuse, intentional and inadvertent is a gaping hole in network security. This results mainly from human error, carelessness and in some case maliciousness. This removes human error from the security equation. Our paper will examine all the technological and feasibility aspects as well as the practical applications. We will look at many different biometric methods of identifying the user.

The presentation has been divided into the following areas:

The presentation highlights the need of biometric pattern matching in our day-to-day lives, how the system works, and different identification methodologies like the fingerprint identification, hand geometry, iris scanning, retinal scanning etc. Besides single biometric identification based on a multi-modal form of biometrics system or multiple biometrics represents an emerging trend.

In this presentation we focus on fingerprint matching and its practical implementation where we compare two fingerprints and display whether they are equal or not. Among all the biometric techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications.

Keywords: Pattern matching, Biometrics.

1. INTRODUCTION

A biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified.

Depending on the context, a biometric system can be either a verification (authentication) system or an identification system In computer technology, biometrics relates to identity-confirmation and security techniques that rely on measurable, individual biological characteristics. For example, fingerprints, handprints, or voice patterns might be used to enable access to a computer, to a room, or to an electronic commerce account. Biometrics is used to identify people based on their biological traits. This growing technological field has deep implications because proving identity is becoming an integral part of our daily lives.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

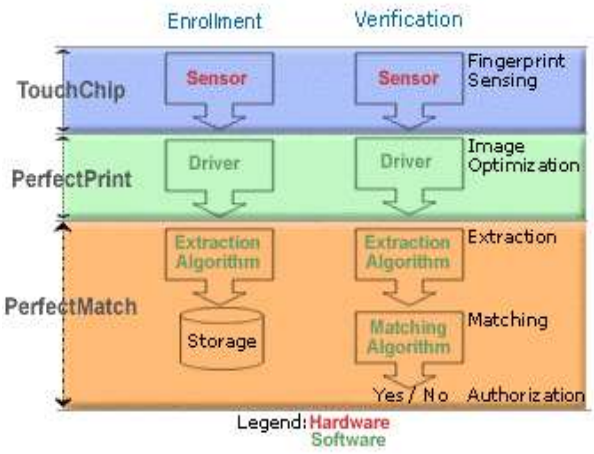
www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

2. HISTORY OF BIOMETRICS

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).

The concept of biometrics probably began with the human use of facial features to identify other people. One of the most well-known biometrics characteristics is the fingerprint. British scientist Sir Francis Galton proposed the use of fingerprints for identification purposes in the late 19th century. He wrote a detailed study of fingerprints, in which he presented a new classification system using prints of all ten fingers, which is the basis of identification systems still in use. British police official Sir Richard Edward Henry introduced fingerprinting in the 1890s as a means of identifying criminals. Automatic fingerprint-based identification systems have been commercially available since the early 1960s. Until the 1990s these systems were used primarily by the police and in certain security applications



Personal Identification Numbers (PINs) were one of the first methods used for identification. There are also methods that involve passwords and physical tokens e.g. smart cards. There are a number of problems associated with this kind of identification. People forget passwords, lose tokens, reuse passwords, write them down, tokens can get stolen. The recognition of the above does not mean the identification of the person providing it - they could be presented by anybody.. This results in a deluge of passwords and means of access, which are often forgotten, misused or lost. With the increased population accessing these networks the risk of attacks on the networks is increased. Companies are turning to Biometrics Systems to bring tighter security to their computer networks.

How the system works?

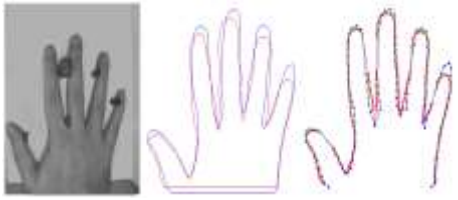
An ideal biometric characteristic should be universal, unique, permanent, and collectable. A characteristic is universal when every person possesses it. A characteristic is unique when no two persons share exactly the same manifestation of the characteristic. A permanent characteristic is one that does not change and cannot be altered. A collectable characteristic is one that a sensor can easily measure. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system In practice, a characteristic that satisfies all the above requirements may not always be usable for a practical biometric system. The designer of a practical biometric system must also consider other issues, such as performance, accuracy, speed, and cost. Two other issues that must be considered are acceptability—the extent to which people are willing to accept a particular biometric identifier in their daily lives—and circumvention—how easy it is to fool the system through fraud.

Popular biometrics methodologies:

You will see reference to a number of biometrics, some of which are rather impractical even if technically interesting. The ‘popular’ biometrics seems to gravitate at present around the following methodologies.

3. FINGERPRINT IDENTIFICATION

Human beings have used fingerprints for personal identification for centuries, and they have used them for criminal investigations for more than 100 years. The validity of fingerprints as a basis for personal identification is thus well established.



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any one individual remain unchanged throughout life. Fingerprints are so distinct that even the prints of identical twins are different. The prints on each finger of the same person are also different.

The level of detail in fingerprint images scanned into a biometric system depends on several factors. They include the amount of pressure applied to the fingertip during image scanning, the presence of any cuts or other deformities on the fingertip, and the dryness of the skin. Therefore, any unusual or prominent features on a fingertip, the endings of the fingerprint ridges, and ridge bifurcations, or branches—collectively known as minutiae—are all used in a biometric system based on fingerprint identification.

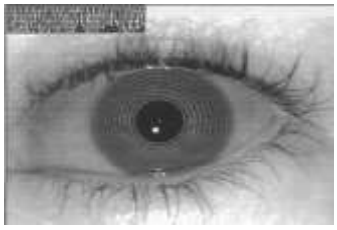
The development of solid-state sensors for fingerprint scanning may soon make the cost of incorporating a fingerprint-based biometric device affordable in many applications, such as laptop computers and cellular telephones. Consequently, researchers expect fingerprint identification to be the leading biometric technique in the near future. One problem with fingerprint technology is its acceptability in society, because fingerprints have traditionally been associated with criminal investigations and police work. Another problem is that the fingerprints of a small fraction of the population may be unsuitable for automatic identification because the prints may be deformed as a result of aging, some genetic condition, or environmental reasons.

Hand Geometry:

A variety of measurements of the human hand can be used as biometric characteristics. These include hand shape, the lengths and widths of the fingers, and the overall size of the hand. Biometric devices based on hand geometry have been installed at many locations around the world. The hand-geometry technique is simple, relatively easy to use, and inexpensive. The main disadvantage of this technique is that it does not distinguish well between the hands of different people. In other words, the system can easily determine if a particular hand shape belongs to a specified individual but cannot reliably determine if a particular hand shape belongs to one of several individuals. Hand geometry information may vary over the lifespan of an individual, especially during childhood, when rapid growth can drastically change hand geometry. In addition, the presence of jewelry or limited dexterity as a result of arthritis may make it difficult for a system to extract correct hand geometry information. Biometric systems based on hand geometry are large in size, so they cannot be used in applications with limited space, such as laptop computers.

4. IRIS-BASED IDENTIFICATION

The iris is the colored part of the eye. It lies at the front of the eye, surrounding the pupil. Each iris is unique, and even irises of identical twins are different. The complex structure of the iris carries distinctive information that is useful for identification of individuals.



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

Early results of research on the accuracy and speed of iris-based identification have been extremely promising. These results indicate that it is feasible to develop a large-scale recognition system using iris information. Furthermore, the iris is more readily imaged than the retina.

Retinal Pattern Recognition

The retina is the innermost layer of the eye. The pattern formed by veins beneath the surface of the retina is unique to each individual. This pattern is a reliable biometric characteristic.

Researchers acquire digital images of retinal patterns by projecting a low-intensity beam of visible or infrared light into a person's eye and scanning an image of the retina. For a fixed portion of the retina to be used for identification, the person undergoing the scan must gaze into an eyepiece and focus on a predetermined spot.

The amount of user cooperation required for a retinal scan makes this technique unacceptable in many applications. On the other hand, a large number of biometric devices based on retinal scans have been installed in prisons and other highly secure environments. The primary disadvantage of this biometric technique is that retinal scanners are expensive.

5. FACIAL RECOGNITION

The most familiar biometric technique is facial recognition. Human beings use facial recognition all the time to identify other people. As a result, in the field of biometrics, facial recognition is one of the most active areas of research. Applications of this research range from the design of systems that identify people from still-photograph images of their faces to the design of systems that recognize active and changing facial images against a cluttered background. More advanced systems can recognize a particular individual in a videotape or a movie. Researchers base the patterns used for facial recognition on both specific and general features. The specific features include the location and shape of facial attributes such as the eyes, eyebrows, nose, lips, and chin. More generally, they employ an overall analysis of the facial image and a breakdown of the image into a number of component images. Researchers are unsure whether the face itself, without any additional information, is sufficient for the accurate recognition of one person in a large group of people. Some facial recognition systems impose restrictions on how the facial images are obtained, sometimes requiring a simple background or special lighting.

Signature Recognition:

Each person has a unique style of handwriting and, therefore, a unique signature. One problem with signature recognition is that the signature of a particular individual may vary somewhat. Despite the variations, researchers have designed a few successful systems for signature-based authentication. Biometric devices based on signature verification are reasonably accurate, but not accurate enough to recognize specific individuals in a large population. However, signature verification is reliable enough to be used in place of a PIN in accessing automated teller machines (ATMs).

There are two approaches to identification based on signature verification: static and dynamic. Static signature verification uses only the geometric (shape) features of a signature, such as the degree of slant, breadth and height of letters, and space between lines, letters, and words. Dynamic signature verification uses both geometric features and dynamic features, such as the speed a person writes and the pressure of the writing implement. Dynamic verification requires a special pen. It is resistant to forgery, as it is virtually impossible for a forger to replicate both the shape of a

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

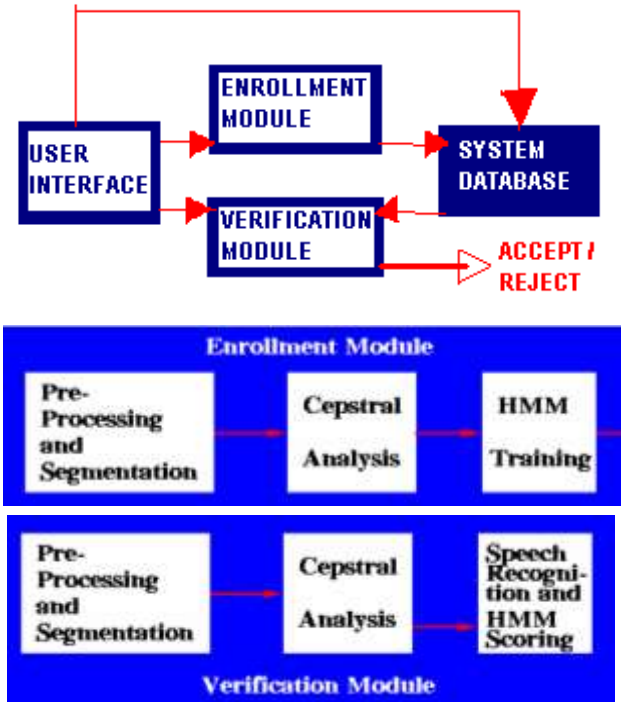
www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

signature and the speed and pressure with which another person signs his or her name. An inherent advantage of a signature-verification system is that the signature is already an acceptable form of personal identification.

6. SPEAKER VERIFICATION

The speaker-specific characteristics of speech are due to differences in physiological and behavioral aspects of the speech production system in humans. The main physiological aspect of the human speech production system is the vocal tract shape. The vocal tract is generally considered as the speech production organ above the vocal folds, which consists of the following: (i) laryngeal pharynx (beneath the epiglottis), (ii) oral pharynx (behind the tongue, between the epiglottis and velum), (iii) oral cavity (forward of the velum and bounded by the lips, tongue, and palate), (iv) nasal pharynx (above the velum, rear end of nasal cavity), and (v) nasal cavity (above the palate and extending from the pharynx to the nostrils). The shaded area in figure 1 depicts the vocal tract.



The vocal tract modifies the spectral content of an acoustic wave as it passes through it, thereby producing speech. Hence, it is common in speaker verification systems to make use of features derived only from the vocal tract.

Multi biometrics:

An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements. I.e. a biometric system, which relies only on a single biometric identifier in making a personal identification, is often not able to meet the desired performance requirements Face recognition is fast but not reliable while fingerprint verification is reliable but inefficient in database retrieval. We have developed a prototype biometrics system, which integrates faces and fingerprints. The system overcomes the limitations of face recognition systems as well as fingerprint verification systems.

Identification based on multiple biometrics represents an emerging trend. This system takes advantage of the capabilities of each individual biometric. It can be used to overcome some of the limitations of a single biometrics.

Examples:

- Integrating Faces and Fingerprints for Personal Identification.
- A Multimodal Biometric System Using Fingerprint, Face, and Speech.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

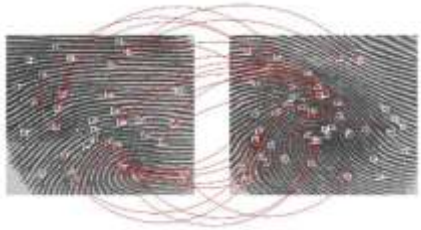
Vol. 03, Issue 07, July 2023, pp : 241-250

7. FINGERPRINT ANALYSIS

Fingerprint Identification:

Human beings have used fingerprints for personal identification for centuries, and they have used them for criminal investigations for more than 100 years. The validity of fingerprints as a basis for personal identification is thus well established. A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any one individual remain unchanged throughout life. Fingerprints are so distinct that even the prints of identical twins are different. The prints on each finger of the same person are also different. The level of detail in fingerprint images scanned into a biometric system depends on several factors. They include the amount of pressure applied to the fingertip during image scanning, the presence of any cuts or other deformities on the fingertip Therefore, any unusual or prominent features on a fingertip, the endings of the fingerprint ridges, and ridge bifurcations or branches—collectively known as minutiae—are all used in a biometric system based on fingerprint identification. The development of solid-state sensors for fingerprint scanning may soon make the cost of incorporating a fingerprint-based biometric device affordable in many applications, such as laptop computers and cellular telephones. Consequently, researchers expect fingerprint identification to be the leading biometric technique in the near future. One problem with fingerprint technology is its acceptability in society, because fingerprints have traditionally been associated with criminal investigations and police work. Another problem is that the fingerprints of a small fraction of the population may be unsuitable for automatic identification because the prints may be deformed as a result of aging, some genetic condition, or environmental reasons.

Fingerprint Matching:



Among all the biometric techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge-ending. Fingerprint matching techniques can be placed into two categories: minutae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

Fingerprint Pattern Types

Fingerprints are the result of minute ridges and valleys found on the hand of every person. In the fingers and thumbs, these ridges form patterns of loops, whorls and arches.

Loop

In a loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered.

Whorl

In a whorl pattern, the ridges are usually circular.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 241-250

Arch

In an arch pattern the ridges enter from one side, make a rise in the center and exit generally on the opposite side

8. IMPLEMENTATION

In this presentation we have implemented the program for matching of two fingerprints using two TIF files (Tagged Image File format) of 100x100 resolution in c and c++. Program results in whether the two fingerprints are equal or not.

The comparison of two fingerprints:

```
int compare(int *img1[100],int *img2[100])
{
int i,j,k=0,l=0,flag,m=0,ct=0,n=0,count=0;
for(i=0;i<=60;i+=20)
for(j=0;j<=60;j+=20)
{
if(ct==1) k=0;
for(;k<=60;k+=20)
{
if(ct==1)  l=0;
for(;l<=60;l+=20)
{
ct=0;
for(m=0;m<20;m++)
{
for(n=0;n<20;n++)
{
if(img1[i+m][j+n]!=img2[k+m][l+n])
{
ct=1;break;
}
}//for n
if(ct==1)  break;
}//for m
if(ct==0) break;
}//for l
if(ct==0)
{
count++; break
}
}//for k
}//for j
```

Applications:

The bulk of biometric applications to date are probably in areas that you will never hear of. This is because there are a very large number of relatively small security related applications undertaken by specialist security systems suppliers. These systems account for the majority of unit sales as far as the device manufacturers are concerned and are often supplied via a third party distribution chain.

The applications that you will here of are those in the public domain. These include:

- ✓ Prison visitor systems, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit - a familiar occurrence among prisons worldwide.
- ✓ Driver's licenses, whereby some authorities found that drivers (particularly truck drivers) had multiple licenses or swapped licenses among themselves when crossing state lines or national borders.

- ✓ Canteen administration, particularly on campus where subsidized meals are available to bona fide students, a system which was being heavily abused in some areas.
- ✓ Benefit payment systems. In America, several states have saved significant amounts of money by implementing biometric verification procedures. Not surprisingly, the numbers of individuals claiming benefit has dropped dramatically in the process, validating the systems as an effective deterrent against multiple claims.
- ✓ Border control. A notable example being the INSPASS trial in America where travelers were issued with a card enabling them to use the strategically based biometric terminals and bypass long immigration queues. There are other pilot systems operating in SE Asia and elsewhere in this respect.
- ✓ Voting systems, where eligible politicians are required to verify their identity during a voting process. This is intended to stop 'proxy' voting where the vote may not go as expected.

In addition there are numerous applications in gold and diamond mines, bullion warehouses and bank vaults, as indeed you might expect, as well as the more commonplace physical access control applications in industry.

9. FUTURE APPLICATIONS-SOME COMMON IDEAS

There are many views concerning potential biometric applications, some popular examples being;

- ATM machine use:
- Workstation and network access:
- Travel and tourism:
- Internet transactions:
- Telephone transactions:
- Public identity cards:

10. DRAWBACKS OF BIOMETRICS

Several countries, including Australia, Canada, the United States and New Zealand, have witnessed public disquiet over identification schemes. Some of the fears that have been cited include:

- That people will be de-humanized by being reduced to codes
- That the system will enhance the power over individuals of particular organizations and the State
- That high-integrity identification embodies an inversion of the appropriate relationship between the citizen and the State
- That the system is a hostile symbol of authority
- That society is becoming driven by technology-assisted bureaucracy, rather than by elected government
- That exemptions and exceptions will exist for powerful individuals and organizations, and that the system will entrench fraud and criminality
- That such identification schemes are the mechanism foretold in religious prophecy (e.g. 'the Mark of the Beast').

11. CONCLUSION

The coming years are going to witness is giant expansion in hardware software changing conventions of speed on a much broader spectrum. Security will become a critical issue and there will definitely a need to protect data from unauthorized users in much efficient ways. Hence biometrics techniques will span the entire information globe irrespective of the increased costs when compared to level of security they offer.

12. REFERENCES

[1] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042- 023-15926-5

[2] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., & Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[3] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[4] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., & Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[5] VenkateswaraRao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., & Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE.

[6] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583- 021X), 2(1).

[7] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07), 2020.

[8] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers.In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409).IEEE. [15]

[9] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE. [17] Vellela, S. S., Basha Sk, K., & Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[10] Rao, M. V., Vellela, S. S., Sk, K. B., Venkateswara, R. B., & Roja, D. (2023). SYSTEMATIC REVIEW ON SOFTWARE APPLICATION UNDERDISTRIBUTED DENIAL OF SERVICE ATTACKS FOR GROUP WEBSITES. Dogo Rangsang Research Journal UGC Care Group I Journal, 13(3), 2347-7180.

[11] Sk, K. B., & Vellela, S. S. (2019). Diamond Search by Using Block Matching Algorithm. DIAMOND SEARCH BY USING BLOCK MATCHING ALGORITHM", International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[12] Sk, K. B., Vellela, S. S., Yakubreddy, K., & Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. Khader Basha Sk, Venkateswara Reddy B, Sai Srinivas Vellela, Kancharakunt Yakub Reddy, M Venkateswara Rao, Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation, 10(3).

[13] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., & Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[14] S Phani Praveen, Rajeswari Nakka, Anuradha Chokka, Venkata Nagaraju Thatha, Sai Srinivas Vellela and Uddagiri Sirisha, “A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques” International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[15] Vellela, S. S., Sk, K. B., & Reddy, V. (2023). Cryonics on the Way to Raising the Dead Using Nanotechnology.

[16] Vellela, S. S., Roja, D., Reddy, V., Sk, K. B., & Rao, M. V. (2023). A New Computer-Based Brain Fingerprinting Technology.

[17] Dalavai, L., Javvadi, S., Sk, K. B., Vellela, S. S., & Vullam, N. (2023). Computerised Image Processing and Pattern Recognition by Using Machine Algorithms.

[18] Vellela, Sai Srinivas and Basha Sk, Khader and B, Venkateswara Reddy and D, Roja and Javvadi, Sravanthi, MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE (June 14, 2023). International Journal of Emerging Technologies and Innovative Research, Vol.10, Issue 6, page no. ppd851-d859, June12023, http://www.jetir.org/papers/JETIR2306410.pdf, Available at SSRN: https://ssrn.com/abstract=447810

[19] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[20] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi1Supervised Learning Approach for Network Intrusion Detection System Based on the ‘GOA’. Journal of Interconnection Networks, 2143047.

[21] Venkateswara Reddy B , SaiSrinivasVellela , KhaderBashaSk , RojaD , KancharakuntYakubreddy , M VenkateswaraRao, Conceptual Hierarchies for Efficient Query Results Navigation, International Journal of All Research Education and Scientific Methods (IJARESM),ISSN: 2455-6211 Volume 11, Issue 3, March-2023,DOI:https://doi.org/11.56025/IJARESM.2023.11323578. http://www.ijaresm.com/conceptual-hierarchies-for-efficient-query-results-navigation

[22] Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[23] Pratap, V. K. (2020). An Effective Automatic Automobile Safety Method Using AI and Convolutional Neural Network. International Journal for Innovative Engineering and Management Research, 9(09).

[24] Gajjala Buchi Babu, Mutyala Venu Gopal, Vellala Sai Srinivas, V. Krishna Pratap, Efficient Key Generation for Multicast Groups Based on Secret Sharing, (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 4, pp.1702-1707.

[25] Vellela, Sai Srinivas and Chaganti, Aswini and Gadde, Srimadhuri and Bachina, Padmapriya and Karre, Rohiwalter, A Novel Approach for Detecting Automated Spammers in Twitter (June 7, 2022). Mukt Shabd Journal Volume XI, Issue VI, JUNE/2022 ISSN NO : 2347-3150, pp. 49-53 , Available at SSRN: https://ssrn.com/abstract=4490635

[26] Vellela, Sai Srinivas and D, Roja and B, Venkateswara Reddy and Sk, Khader Basha and Rao, Dr M Venkateswara, A New Computer-Based Brain Fingerprinting Technology (June 18, 2023). International Journal Of Progressive Research In Engineering Management And Science, Vol. 03, Issue 06, June 2023, pp : 247-252 e-ISSN : 2583-1062., Available at SSRN: https://ssrn.com/abstract=4483497

[27] Vellela, Sai Srinivas and Sk, Khader Basha and B, Venkateswara Reddy, Cryonics on the Way to Raising the Dead Using Nanotechnology (June 18, 2023). INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS), Vol. 03, Issue 06, June 2023, pp : 253-257, Available at SSRN: https://ssrn.com/abstract=4483499

[28] Vellela, Sai Srinivas and Basha Sk, Khader and B, Venkateswara Reddy and D, Roja and Javvadi, Sravanthi, MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE (June 14, 2023). International Journal of Emerging Technologies and Innovative Research, Vol.10, Issue 6, page no. ppd851-d859, June-2023, http://www.jetir.org/papers/JETIR2306410.pdf, Available at SSRN: https://ssrn.com/abstract=4478104

[29] D, Roja and Dalavai, Lavanya and Javvadi, Sravanthi and Sk, Khader Basha and Vellela, Sai Srinivas and B, Venkateswara Reddy and Vullam, Nagagopiraju, Computerised Image Processing and Pattern Recognition by Using Machine Algorithms (April 10, 2023). TIJER International Research Journal, Volume 10 Issue 4, April 2023, Available at SSRN: https://ssrn.com/abstract=4428667

[30] Vellela, Sai Srinivas and Pushpalatha, D and Sarathkumar, G and Kavitha, C.H. and Harshithkumar, D, Advanced Intelligence Health Insurance Cost Prediction Using Random Forest (March 1, 2023). ZKG International, Volume VIII Issue I MARCH 2023, Available at SSRN: https://ssrn.com/abstract=4473700

[31] K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. Khader Basha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.