International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-107 PAGE NO: 620-624.

# ADVANCED POLLING BY IRIS TECHNOLOGY WITH CLOUD COMPUTING AND GAIC ALGORITHM USING BIOMETRIC SECURITY

**C.Thirumoorthi**
*Assistant Professor, PG and Research Department of Computer Applications,*
*Hindusthan College of Arts and Science, Coimbatore.*
cthirumoorthymca@gmail.com

***Abstract*— Unlike other biometrics such as fingerprints and face, the distinct aspect of iris comes from randomly distributed features. This leads to its high reliability for personal identification, and at the same time, the difficulty in effectively representing such details in an image. This paper describes efficient algorithm for iris recognition by characterizing key local variations. The basic idea is that local sharp variation points, denoting the appearing or vanishing of an important image structure, are utilized to represent the characteristics of the iris. The whole procedure of feature extraction includes two steps:1) A set of one-dimensional intensity signals is constructed to effectively characterize the most important information of the original two-dimensional image; 2) Using a particular class of wavelets, a position sequence of local sharp variation points in such signals is recorded as features. A fast matching scheme based on exclusive OR operation to compute the similarity between a pair of position sequences. The process of data collection acquired through the ocean of cloud computing, analyzed in cluster analysis and applied with the various data mining techniques to extract the needed data. As many as 15 types of identifications schemes are used in general elections nowadays. So the rate of interchange is high. But, this can be avoided by our new innovative possible technological trend of implementing "IRIS SCANNING MECHANISM". Iris is the colored part of the eye that consists of a muscular diaphragm surrounding the pupil and regulating the light entering the eye by expanding and contracting the pupil. As the ratio of people having same iris structure is 10^78 it have adopted this mechanism. Thus providing biometric security, it signs to bring secured democracy in our nation.**

***Index Terms*—Biometric security, Data mining, Cloud Computing, IRIS Scanning Mechanism, Fingerprint, GAIC Algorithm**

## 1. INTRODUCTION

Biometrics is the science of measuring an individual's Physiological or behavioral characteristics for automatic identification. Biometrics is the only viable approach to personal recognition. It can give automatic Personal recognition based on physiological or behavioral characteristics. Any human Biometric character satisfies Universality, Distinctiveness, Permanence and Collectiveness.

So, Biometry can be the only way for offering greater security and convenience than traditional methods of personal recognition.

The recognition of person by his Fingerprint, Face, Hand geometry, Iris scanning and Voice recognition.

## 2. CLOUD COMPUTING- AN OVERVIEW

The improvements in the science field results in the management of huge data that are computerized and stored in databases. The stored data contains hidden knowledge that is very important and useful for many decision making approaches. The conventional statistical methods which are not possible to unravel this knowledge and are also time consuming. Moreover, it may produce improper conclusions ultimately affect decision making. So it is an essential need to collect the appropriate data and made used over efficient techniques to arrive with the better solutions.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-107 PAGE NO: 620-624.

*2.1. Cloud computing vs. Internet technologies.*

Cloud computing is said to be a mode of delivering hardware, software or services on a virtualized and scalable platform using Internet technologies. It enables client organizations to have access to highly available services with charges that vary based on utilization. It eliminates the organizations to invest on highly expensive technological equipment's and minimizes the risk. The services of a cloud computing can be provided to the users in three major categories such as software, platform and the infrastructure. Now in the field of technology the cloud computing is said to be a great beneficiary for obtaining a large scale of data. It is benefit because of its qualities such as paying according the usage, instant scalability, security, reliability etc.,

## 3. Biometric Authentication Mechanism

Biometric Authentication is defined as measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, identification for a specific user can be determined and authentication for access can be granted.

*3.1 Iris scans*

Iris recognition creates an "eye signature" from the vascular configuration of the iris, an extremely consistent and reliable attribute with the advantage of being protected inside the eye itself. An image of iris is captured by having the individual look through a lens at the alignment target. Diseases or injuries that would interfere with the iris are comparatively rare in the general population.

*3.2 Iris*

Eye is the precious part of the body with the diameter of 20 mm. It consists of outer sclera, cornea, and the choroids ant the retina. Choroids are below sclera formed by the blood vessels and are pigmented. The anterior choroids are divided into *ciliary body* and *iris diaphragm*. Iris has the capability of expansion and contraction. It maintains the lens in the perfect cavity. Lens contains 60-70% of water and 7% of fat with more proteins. Optometrist research suggested that the patterns of blood vessels on the back of the human eye were unique from person to person. Further research resulted that these patterns, even between identical twins, were indeed unique throughout the iris.

More specifically the surveys say that ***1:10^78*** will have the same type of iris which is the rarity case of error occurrence. This can be avoided by the blood vessel detection.

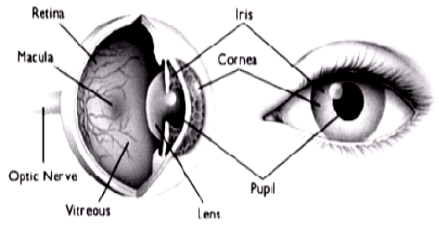


Fig. 1: Iris technology

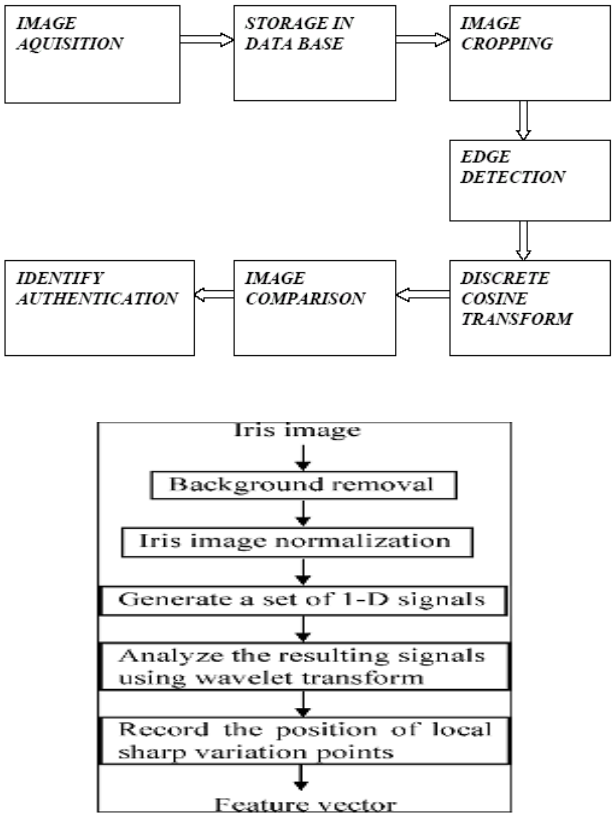


Fig. 2: Block diagrams

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-107 PAGE NO: 620-624.

## 4. Image Cropping

The eye consists of the factor called the resolution. This is of two types.

Spatial: This is related with the sampling interval. High spatial resolution, more sampling rate and increase in the sampling point

Gray level: This depends on the quantization level. More quantization levels results in the lower quantization error.

The test image is converted to the gray level scale. Then the image is cropped i.e. the needed information is taken from the tested image.

### *4.1 Edge Detection*

Boundary between two regions with relatively gray level properties will form an edge. Pixel locations of abrupt gray level change are noted. Many local derivative operators are used to detect the edge points. Edge detection can be made using the gradient operators. Many types of the operators are available. The highly contented is the sobel operator and prewitt operator. Thus the edge detection of the test image is done.

### *4.2 Image Transformation*

The image obtained is to be converted into the mathematical form so as to make the comparison with the first image that is obtained already. So the test image is transformed using any of the types- DFT, FFT, Walsh, Hadamard, DCT, Haal, Slant, and Hotelling. Discrete cosine transform can be suggested because information packing is superior; basis images of DCT are fixed. The process of the image transformation is done to the test image. Then the first image is cropped, edge detected and transformed using the cosine transform.

### *4.3 Image Comparison*

Then the image comparison between the test and first image is made. The grant and denial of the process is made by this process. The transform of the test image is compared with the every first image in the data base. If the match is found in the database the person's information is displayed and he's allowed to cast his vote. Else he's rejected for voting.

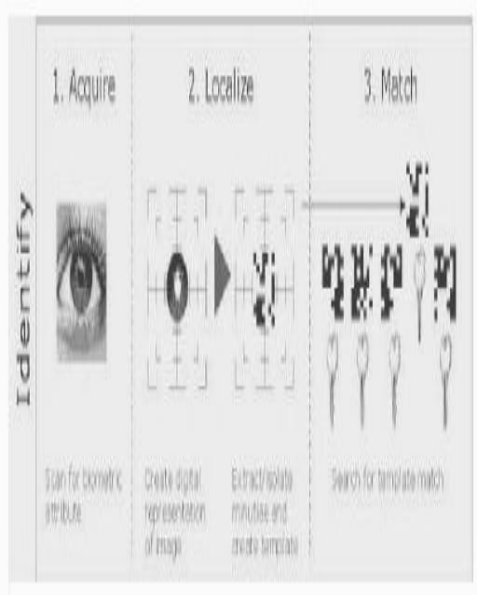


Fig 3: Identification and Authentication

## 5. Minimization Of FAR

The false acceptance rate (FAR) can be adjusted in the recognition algorithm via the acceptance threshold - the higher the acceptance threshold, the lower the FAR. Raising the acceptance threshold, however also raises the FRR. Therefore, the goal must be to have as small an FAR as possible for any given FRR, and vice versa.

There are certain factors, which primarily influence the FAR, while others mainly affect the FRR. For a fixed FRR, FAR is dependent on the following factors:

- Type of biometric feature (retina in this case)
- Quality of the sensors
- User behavior
- Effectiveness of the recognition algorithm
- The number of biometric references in an identification.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-107 PAGE NO: 620-624.

## 6. Data Mining – an Opt Technique

One challenge to law enforcement and intelligence agencies is the difficulty of analyzing large volumes of data involved in criminal and terrorist activities. Data mining holds the promise of making it easy, convenient, and practical to explore very large databases for organizations and users. *Crime* is defined as "an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law". Data mining is used for the identification of those data, where the overall data designates patterns, statistical or predictive models of the data, and relationships among parts of the data. Data mining in the context of crime and intelligence analysis for national security is still a young field.

### *6.1. Online Access*

In the general election process, the voter should bring the identity card or citizenship card to the election booth. The concerned authorities check these authorized identity cards. In case both databases are same, the voter is checked for already polling in the same election the voter is sent to poll. In the EVM the voter poll for his / her desired party. Since this is a time consuming and unreliable process.

Further the government has to pay extra wages for the servants. In the actual implementation process, the voter should stand before the retina scanning device system; the system acquires an image of the attribute through an appropriate scanning technique. Once the scanned content is acquired, it must be localized (in the server & user database) for processing purposes.

The localization is actually encrypted in GAIC algorithm (so that unauthorized user can't access). During this step, extraneous informational content is discarded and minutiae are isolated and turned into a template (cryptographic algorithm), a sort of internal canonical form for matching attributes stored in a database. Minutiae are the uniquely differentiating characteristics of the biometric attribute. The scanned template of that person is checked with all other templates. if the exact match is found, then the database is checked whether he has already voted on the same election, if not, then the concerned voter D-base is published (saying eligible to vote).

The voter can poll for his / her desired party. In case, if a voter tries to vote for once again, it can't be done. Our Algorithm made a sweep for that because once polling is done; an entry is made in to the voter's Database. This prevents the malpractice of rigging.

#### *6.1.1. Flow Chart for Online Access*

The following flow chart shows the process involved in the authentication of the voter.

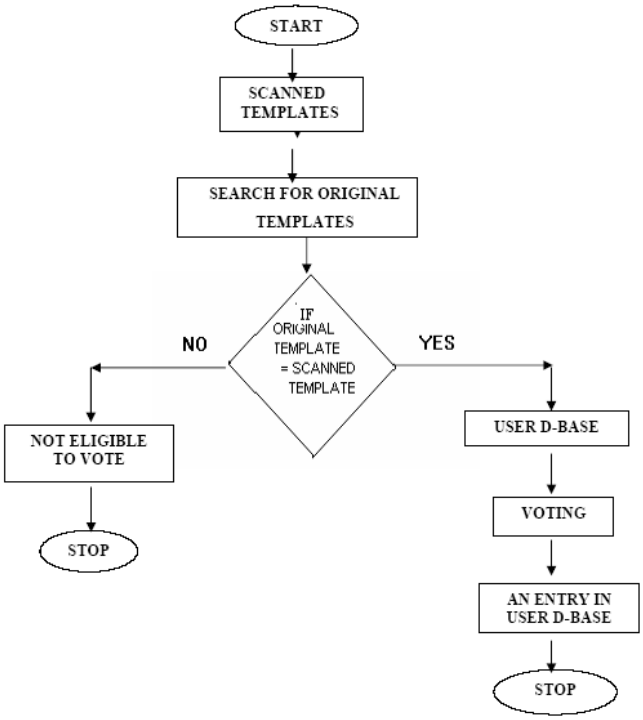


Fig. 4 Steps Followed to Authenticate Voter

## 7. Merits

- This integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a mole verification system etc.
- It meets the response time as well as the accuracy requirements.
- With the exception of some types of degenerative eye diseases or cases of severe head trauma are stable enough to be used throughout one's life.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-107 PAGE NO: 620-624.

- This secure voting system prevents the malpractice like illegal voting, blame of voters etc.
- Since this is an integrated network system, one can put his\her vote from any part in that particular constituency (WAN).

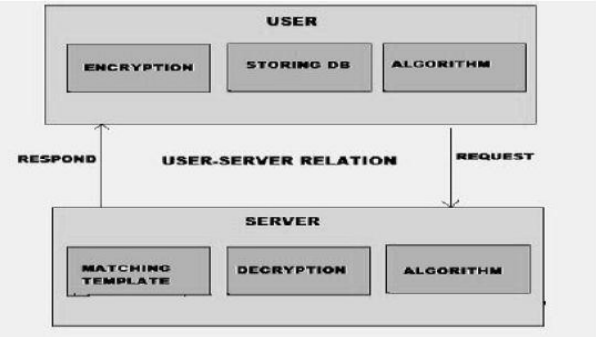


Fig. 5 User and the Server

## CONCLUSION

The increase in malpractices during election polling like rigging, miscreant made us to relay on highly secure polling system. Even though the present EVMPS skips some sort of burden. Still it is not much reliable one. Again through this scheme malpractice is further increased. Implementing the use of information security measures may help in the war against hacking, but people must not forget the basics of computer security. People must do the simple things that make it harder for hackers to get into our computers or systems. This is because biometrics links the event to a particular individual, is convenient, accurate, can provide an audit trail and is becoming socially acceptable for its security.

Hence people surely say that the iris scanning technology is the most prominent one among the biometrics and helps much more in individual's privacy and security, helping thus in online polling system.

## REFERENCES

**[1] C McCue, "Using Data Mining to Predict and Prevent Violent Crimes", available at: http:// www.spss.com/dirvideo/richmond.htm?source=dmp age&zone=rtsidebar.**

**[2]. O. de Vel et al., "Mining E-Mail Content for Author Identification Forensics," SIGMOD Record, vol. 30, no. 4, 2001, pp. 55-64.**

**[3]. G. Wang, H. Chen, and H. Atabakhsh, "Automatically Detecting Deceptive Criminal Identities," Comm. ACM, Mar. 2004, pp. 70-76.**

**[4]. S. Wasserman and K. Faust, Social Network Analysis: Methods and Applications, Cambridge University .Press, 1994.**

**[5]. Chen, H., & Lynch, K.J. (1992). Automatic construction of networks of concepts characterizing document databases. IEEE Transactions on Systems, Man, and Cybernetics, 22(5), 885-902.**

**[6]. de Vel, O., Anderson,40 A., Corney, M., & Mohay, G. (2001). Mining E-mail Content for Author Identification Forensics. SIGMOD Record, 30(4), 55-64.**

**[7] A. Jain, R. Bolle, and S. Pankanti, Eds.,Biometrics: Personal Identification in a Networked Society. Norwell, MA: Kluwer,1999.**

**[8] D. Zhang, Automated Biometrics: Technologies and Systems. Norwell, MA: Kluwer, 2000.**

**[9] T. Mansfield, G. Kelly, D. Chandler, and J.Kane, "Biometric product testing final report," Nat. Physical Lab., Middlesex, U.K., 2001.**

**[10] A. Mansfield and J. Wayman, "Best practice standards for testing and reporting on biometric device performance," Nat. Physical Lab., Middlesex, U.K., 2002.**