Secured Big Data Based on Ocular Recognition

R. Vanithamani, T. Kumanan,

***Abstract** In the last few decades, technology has played a main role in developing the electronic devices sharing data, such as sensors, actuators, individual archives, cloud and social networks. Managing this variety of large data called as big data efficiently is a challenging task. The critical challenge in handling big data is security and privacy. At any stage privacy may not be disclosed. Various existing techniques based on encryption and anonymization for security is not perfectly suitable for the unstructured, high speed, large volume big data. In this paper, analysis and discussion is done on how biometric verification and authentication secures big data. Fingerprint being the well-known biometric, ocular recognition is the most reliable biometric technique compared to iris recognition. The unique feature of human iris is its pattern and color which is identified by the type and amount of the pigment in it. The proposed method combines both iris and retinal authentication technique to provide better security for the big data in the emerging field of Internet of Things (IOT).*

***Keywords:** Big data, Anonymization, Ocular recognition, Iris recognition, Biometric authentication, Mobile security, Digital verification.*

I. INTRODUCTION

A large collection of complex data sets is termed as “Big Data” which is difficult to handle using traditional database management tools or data processing applications. Various challenges of big data are search, transfer, sharing, security, capture, storage and visualization. IBM visualizes how the analysis of single large data set generates addition information leading to large data sets compared to separate smaller data sets of same size. A classic example of big data [1] is the text and images of Wikipedia of the size of multiple terabytes. Security and privacy are the main requirements of handling Big Data. Analysis and measurement of the unique physical features of human body is known as biometrics. A Person can be identified by various physiological biometrics such as fingerprint, facial recognition, eye, handprint and even DNA. The human eye senses information such as textures, shapes, colors and movement and allows the brain to process the information. Ocular recognition [2] could be a great tool for individual identification and authentication. Any technique is convenient based on its ease of use [3]. For example Android and Apple smart phones are unlocked by recognizing the finger print of the user and also used in banking applications [4]. The main aspect of the modern society is security, as the users hold on different devices and communication techniques [5].

Ocular recognition is rarely applied in the security domain inspite of its promising privacy in the IOT market [6]. In this paper, analysis is done on security and authentication of the Ocular recognition for the big data.

Authenticating an unauthorized user to access the data is literally not possible with Ocular recognition. The mechanism of security and convenience provided by Ocular recognition enables a new way of authenticated users via smart phones. Big data authenticated with Ocular recognition provides an opportunity for making decisions providing new way for business and commercial sectors of society.

II. BIG DATA AND ITS SECURITY

A variety of high velocity large volume information which can be unstructured, semi structured or structured needs to be processed for enhanced decision making and optimization of process. For the existing technology big data is very huge, very fast and tough for storage along with processing. Data size is more than Peta Byte equivalent to 1000 Tera Byte. Based on the analysis big data provides an opportunity for making decisions. The existing system of data sampling and data processing is not sufficient for providing accurate results for big data. Sampling the data of social network and processing leads to inaccurate analysis. The current digitization of data, internetworking and machine people interaction leads to a large volume of diverse data called as big data. Hence big data means more operation, more communication and more observation leading to higher profit margins creating impact on all economical sectors. Securing this large volume of data and to provide ultimate privacy is the current requirement. The proposed method focuses on implementing Ocular recognition to secure big data. Currently there is no software or hardware specifically for Ocular recognition but the same exist for Iris recognition or Retinal scanning. Ocular recognition being a hybrid system combines Iris recognition and retinal recognition for authentication a user has a different framework. The iris of the human eye is scanned, applied to certain algorithms such as Log Gabor, SVM etc. to authenticate the person based on the information in the database as in Fig.1. The biggest player Samsung Unlocks the smart phone by recognizing the iris of the user [7]. The companies need to manufacture their own software and hardware suitable for iris recognition authentication for big data, or purchase it from a third party company.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

R. Vanithamani*, Research Scholar/Computer Science, MAHER University

Dr. T. Kumanan, Professor/Computer Science, MAHER University

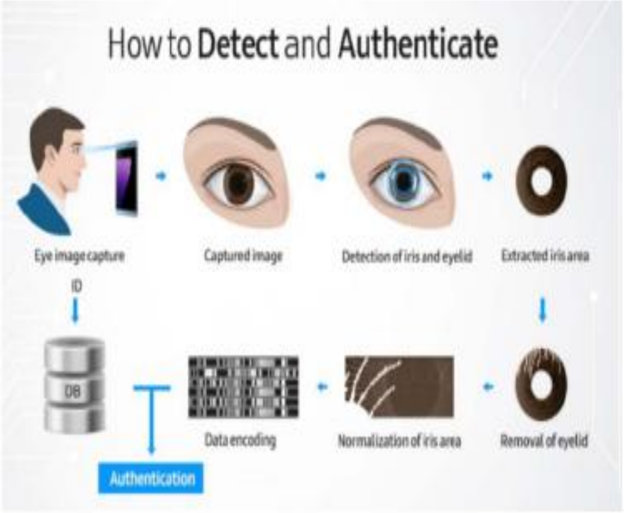


Fig.1. Process of Iris Recognition

Retinal scanning involves scanning of illuminated blood vessels, white spaces from the human eye and quiet different from iris recognition. Big corporate companies requiring high security for their data prefer retinal scanning than iris recognition. The major issue of retinal scanning is its cost and complexity [8]. Table I shows the Comparison of various biometric techniques.

Table 1 Crossover Accuracy of Biometrics

Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50

III. CHALLENGES OF BIG DATA

Following are the challenges of big data besides its big opportunities: -

A. Storage challenge

The basic challenge of big data is its volume and creating a sustainable system for storage. Secondly identifying data set worth storing on the device from the data flood, stored securely, improves the processing speed and retrieval. One of the biggest challenges of big data is to handle the meta-data and cleaning the data [1] [9].

B. The challenge of Processing:

Processing the variety of big data from various sources is a challenging task as it may be unstructured, semi-structured, and structured. A new technology is required for handling different data structures and to produce fault free data integration, representation and aggregation [9] [10].

C. Security and Privacy:

Security and privacy of information are the major issues of the current era. A security model which prevents data leakage at processing time and secures from treats during storage of this huge data is required for preserving big data [1] [11] [12].

IV. OCULAR RECOGNITION – FRAMEWORK

Ocular recognition is divided into two segments: Iris recognition and Retinal Scanning due to the complexity of human eye. Retina is a tissue of neural cell situated in the posterior part of the eye. Each human has unique retina [13] as it is a complex structure of capillaries supplying blood to the human eye. Mapping a person's retinal unique pattern is known as retinal scan [13]. This pattern is as unique as even the twins do not have the same pattern. The scanning is done by transmitting infrared light into the eye tracing the path, converted into computer code and stored in a database. The iris is the part of the human eye controlling the pupil size and diameter. Similar to retinal scanning, infrared light gets the images of the iris structure which affects the amount of light passing through retina. Retinal scan & iris recognition are highly reliable since both are unique for a person. The proposed system is based on the identification key containing different sections such as size, shape, color, position and distance between the centres of two eyes.

V. BIG DATA PRIVACY CHALLENGES

The method of preventing the disclosed sensitive information is known as privacy. As big data is of large volume and of different types, it may contain personal information of individuals which needs privacy. Following are the factors playing important roles in the privacy of big data.

A. Privacy Based on Context:

The same data set have different meaning in different context, deciding appropriate meaning in a particular context in challenging. Hence the privacy level of the data set has to be identified.

B. Aggregated and Co-related Data sets:

Big data is correlated data, where each dataset is related to other data set hence disclosing the privacy of one data set leads to the disclosing the privacy of other data set also. As information of one data set is required by other data set also, disclosing of privacy is again a treat for data processing. This correlation and aggregation of big data is referred as Quasi-identifier which acts as a big treat to the privacy of big data.

C. Modeling of Privacy Threat:

The structured and systematic technique of priory identifying the privacy objectives and designing a solution for preserving the privacy is known as threat modeling. To model the threat a clear picture of the type of privacy attack and managing them is required. As the size of big data is huge, designing a solution for the identified threats is not an easy task.

D. Budgeting of Privacy:

Another challenging issue to preserve privacy in big data is cost. As the cost depends on the computational load, choosing a technique that is computationally expensive is not advisable. Hence the proposed technique should provide comparatively efficient computation at lower budget.

VI. PROPOSED METHOD

The primary requirement is to provide security and privacy for big data. Ocular recognition which combines iris recognition and retinal scanning provides the required security for big data. Many efficient and accurate algorithms with different approaches are implemented for iris recognition basic steps being image pre-processing, feature extraction and iris matching.

A. Image Pre-Processing

The image of human eye is segmented to extract the iris image, for this the algorithm must properly locate the inner pupil and limbus outer boundary of the iris. The distance between the iris centre and the pupil centre is accurately determined by the Daugman's algorithm [14] which uses the integro differential operator. An exhaustive search is performed by the integro differential operator by using different circle centers with different radii and locates the local maxima best matching the pupil and iris boundaries [14]. Circular Hough transformation and canny edge detection are used by Masek's algorithm where the canny operator generates a gradient which is the edge map of the eye [15]. Then the edge map is processed by the Hough transformation which detects circular objects matching the parameters of iris or pupil.

B. Feature Extraction:

The important features of the iris is extracted from the image to reduce its size is known as feature extraction. Daugman's algorithm extracts the iris features using wavelet based analysis that uses 2D Gabor filters extracting the phase information of the iris [14]. Information about iris is encoded using these features using binary bit pattern. The Masek's algorithm uses the log Gabor filters ignoring the background and extracts the iris features [16].

C. Matching and Verification:

The statistical independence between the iris codes of Daugman's method is implemented for iris recognition [14]. The extracted encoded image of the iris is taken for finding the hamming distance between the two irises being compared and number of identical bits between the two binary patterns is calculated [14].

VII. IMPLEMENTATION OF PROPOSED METHOD

Ocular recognition is the fusion of iris recognition and retinal scanning. For iris scanning existing algorithm is used whose result is combined with the results of retinal scanning using fusion technology without any interlinking. A unique ID key number is created for each user for communication with third party database.

A. Iris System:

Iris of the user is scanned and the image of the iris undergoes Image Preprocessing, Feature Extraction, Matching and Verification algorithm to generate a unique ID number. Daugman's algorithm is used to implement the iris scanning process. This unique ID number is stored in the database for further matching.

B. Retinal Scanning:

Area match-fusion algorithm is used for retinal scanning which maps out different area of the retina generating specific letters and numbers randomly arranged based on distance between certain factors. Every time the retina is scanned, letters remains the same while the numbers change as different area is scanned every time. Letters are taken as reference and stored in the database along with the numbers for comparison purpose.

C. Fusion of Scan Report:

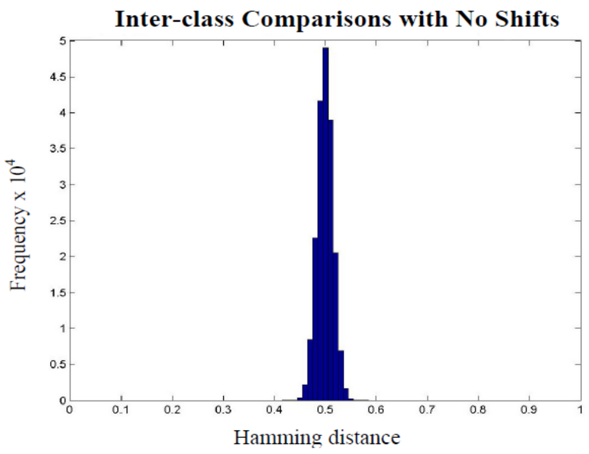
After performing iris scanning and retinal scanning, the report is fused every time and the updated scan result is stored in the database. This scan fusion is maintained separately without linking with iris scan report or the retinal scan report, helping the system to report failure and to maintain accuracy.

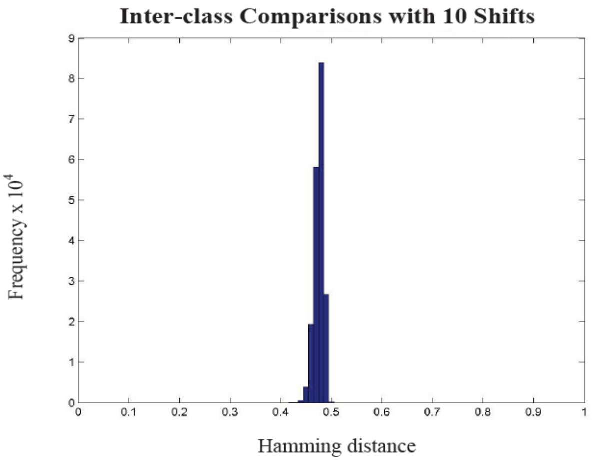
D. Reporting Third-Party Approval:

The scanned results are stored in separate database; a unique ID number is created for each client and reported to third party. As Ocular recognition is authenticated, with the approval of third party the user is allowed to access the big data. The platform is secure as no private data about the client or the vendor is stored in any database.

VIII. DISCUSSION & RESULT ANALYSIS

The proposed method examines the iris and the retina together in order to minimize false matching & false acceptation rate. Experiments were conducted using MATLAB for unique recognition by reduction of degrees of freedom in the ocular template. The parameters for the ocular recognition system are the radial resolution 'r' and angular recognition 'θ' respectively. The number of shifts indicates the inconsistencies in the rotational movement between two different ocular features of the human eye. Uniqueness of the human eye is examined by the comparison of the hamming distance distribution called as interclass distribution. Interclass hamming distribution with no shifts and 10 shifts is simulated as shown in Fig.2. The mean is 0.5 with no shift whereas the mean value is slightly shifted to 0.47 with 10 shifts. Hence as the number of shifts increases, correspondingly the hamming distance decreases indicating the uniqueness. The result obtained involves various parameters of the filter to encode the ocular template. Each data set provides maximum decidability for a optimal central wavelength as shown in Fig.3.





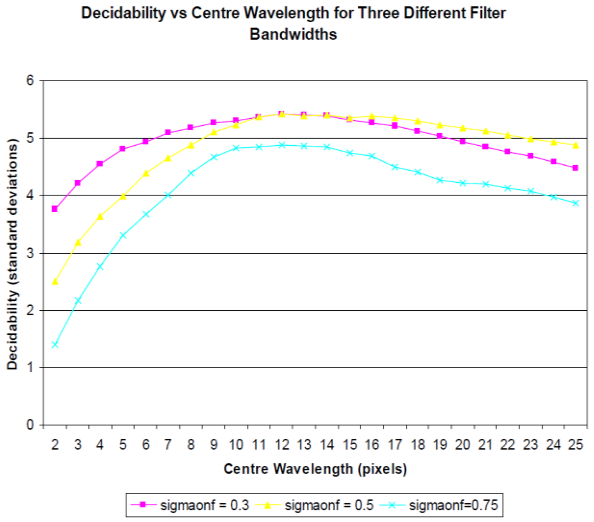


Fig.2. Interclass hamming distribution with no shifts &10 shifts Fig.3. Ocular Decidability Vs Central wavelength

IX. CONCLUSION AND FUTURE WORK

Privacy and security are the critical issues of Big data, faces many challenges due to its extra ordinary scale. Ocular Recognition is the best proven biometric system for authentication should be used widely in IoT domain in the near future. The proposed system of Ocular Recognition for securing big data would be accurate, efficient and cost effective. Analysis and detailed study of Ocular Recognition leads to a conclusion that Ocular recognition technique is capable of meeting most of the challenges of big data. Both client and vendor are beneficial as it works differently for each user. In the future, the proposed method can be implemented in real time applications where authentication, security and privacy are the primary requirements supplementing the theory of current work.

REFERENCES

1. https/cloudsecurityalliance.org/research/big-data.
2. P. Liu, J. M. Guo, S. H. Tseng, K. Wong, J. D. Lee, C. C. Yao, *et al.*, "Ocular Recognition for Blinking Eyes," *IEEE Transactions on Image Processing*, vol. 26, pp. 5070-5081, 2017.
3. R. M. Parizi and A. Shahi, "Component-Driven Development in Modern Virtual Assistants: A Mapping Study," *Journal of Software*, vol. 13, pp.126-137, 2018.
4. A. M. H. Jafar and H. E. Aboul, "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory," *Advanced Modeling and Optimization*, vol. 5, 2003.
5. D. Kiwia, A. Dehghantanha, K.-K. R. Choo, and J. Slaughter, "A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence," *Journal of Computational Science*, 2017.
6. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multichannel communication in Edge-of-Things," *Future Generation Computer Systems*, vol. 85, pp. 190-200, 2018.
7. M. Shuddhahnik. (2017, 14 September 2017). Face ID vs Iris Scanner:Is iPhone X more secure than Galaxy S8? Available:http://www.techradar.com/news/face-id-vs-iris-scanner-is-iphone-xmore-secure-than-galaxy-s8
8. P. Mittal. (2013, 13 October 2017). Retinal Recognition. Available: https://www.slideshare.net/piyushmittalin/retinal-recognition
9. Lu, Rongxing, Hui Zhu, Ximeng Liu, Joseph K. Liu, and Jun Shao. "Toward efficient and privacy-preserving computing in big data era." *Network, IEEE* 28, no. 4 (2014): 46-50.
10. Zhang, Du. "Granularities and inconsistencies in big data analysis."*International Journal of Software Engineering and Knowledge Engineering* 23, no. 06 (2013): 887-893.
11. Hirsch, Dennis D. "The Glass House Effect: Big Data, the New Oil, and the Power of Analogy." *Maine Law Review* 66 (2014): 2.
12. Katal, Avita, Mohammad Wazid, and R. H. Goudar. "Big data: Issues, challenges, tools and Good practices." In *Contemporary Computing (IC3), 2013 Sixth International Conference on*, pp. 404-409. IEEE, 2013.
13. P. Mittal. (2013, 13 October 2017). Retinal Recognition. Available: https://www.slideshare.net/piyushmittalin/retinal-recognition
14. J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 21-30, 2004.
15. D. Rankin, B. Scotney, P. Morrow, R. Mcdowell, and B. Pierscionek, "Comparing and Improving Algorithms for Iris Recognition," presented at the 13th Irish Machine Vision and Image Processing Conference, 2009.
16. S. G, H. Srinivas, and D. NT, "Efficient Iris Recognition by Fusion of Matching Scores obtained by Lifting DWT and Log-Gabor methods of Feature Extraction," *International Journal of Applied Research*, vol. 1, pp. 1067-1073, 2015.