A Novel Review on Biometric System Based on Digital Signal Processing

Divya Jyothi Uppari*

Jawaharlal Nehru Technological University, Hyderabad, Telangana 500085, India

Review Article

Received: 30/07/2016
Revised: 16/08/2016
Accepted: 27/08/2016

***For Correspondence**

Divya Jyothi Uppari
Jawaharlal Nehru Technological University, Hyderabad, Telangana, 500085, India, Tel: +91 9590807049

Keywords: Biometric system, Identification, Security

E-mail: divyauppari@rediffmail.com

ABSTRACT

Biometric system is a device used to identify the individual based on physiological or behavior characteristics. The unique identification can be measured either through fingerprints, facial, eyelids, iris, sound, Heart beat etc. The use of biometric system used in day to day life. The management of the system is to maintain security regarding their need of work. In the present review we just tried to present how the biometric system works and used in daily life.

INTRODUCTION

Biometrics is programmed method to verify or recognize for identification of a living person depending on a physical or behavior characters [1]. This system varies depending on the requirement in other terms it can be purpose, procedures and technologies. But it is utilized by us in our daily life in one or the other way. This review explains about the technology of Biometrics and its application in the present society [2, 3].

This science is basically depends on the human identification of the humans [4]. Biometrics is machine language that can make identification physically. Authentication is carried out by machine or either by digital appearance. We generally observe that collection of finger prints, DNA, hair analysis could not be a part of this system [5, 6, 7]. The collection of data can be manipulated and accuracy can be minimized. The identification of person to person is also difficult. So, Biometric system is useful for the accurate authentication with a quick approach and result [8, 9].

As per the advance technologies this is the improvement is carried out by information technology. This is been observed in our daily life as shown in **Figure 1**.

Figure 1: Biometric system used in daily life.

Biometric system is a technical system which collects data regarding a person (or other biological organism) to identify that person, depending on exact data about unique biological traits which carry out the work efficiently [10-14]. This system would involve ongoing data by an algorithm for exact result, it is connected to identification of a user or other individual. The recognition of the individual can be through finger prints, eye lids, facial, heart beat (advanced) [15-17].

HISTORY

As per the literature in 1870 to identify this humans and notify dates a measuring system is been invented by Alphonse Bertillon. This system is been designed in such a way to measure the diameter of the skull, hand (arm) and length of feet. In 1920, system was been utilized in USA to identify the thieves. During 1880's it was slowly developed to identify by finger prints and through measurements of face. While in 1960 the Digital signal processing is been introduced it has given a good support to identify humans identity easily, extending this technique measurement of hand is also notified [18-24]. By the government interest this system is utilized to identify the pupils. Not only this in 1980,s verification is carried out by retina and signature. This is improved in 1990s to recognize the Iris.

MECHANISM

Components of biometric system

These devices depend on usually different technologies. Biometric system divided into five subsystems: Sensor (as an input), Signal Processing algorithm, Data storage, matching algorithm and Decision process. These subsystems can be considered at once [25-28].

Sensor

The screening of the input is initiated with the help of sensors. This is to assemble data and translate information into digital format. Sensor play a major role collect data such as finger prints, eye lids, facial recognition etc. depending on the requirement [30, 31].

All biometric systems assemble the data at one position but store and process it at other location. System must require data transmission that great amount of data involve, conversion is required to transmit or storage to save bandwidth and space to store. Conversion and transmit can occur before processing signal and store image [32-35].

During the transmission or compressed data to store should be helpful for further use. In the procedure of conversion compression of data is done and expanding may cause quality loss to restore the signal. This can influence the compression ratio. This conversion may be done depending on the signal generated by biometric system. Researcher has designed to convert the unique signal for collected data [36, 37]. It may vary depending on the input. For face it is wavelength scalar quantization, facial images are JPEG format and Code excited linear prediction is done to store voice data.

Signal processing algorithm

Algorithm in the designed in such a way to convert the input data in digital form signal. It makes an easy path to match the data already stored in the system. This plays a crucial role that a template is modified according to registered data. Conversion of this data can be helpful to match the stored data [38].

By obtaining and feasible to transmit a biometric character, preparation should be done to match between other like measure. This divides the signal-processing four tasks such as segmentation, feature extraction, quality control and pattern matching. Segmentation is a process to find the pattern for biometric system to transmit the signal. For example, a facial recognition [39, 40] is made to recognize the boundaries or measures of the face or faces that converted to digital code from image. Sounds can be predicted depending on the wavelength periods, this means the extraction of data is carried out. Extraction of feature is interesting and biometric pattern, segments from the greater signal, covers no repeat alters caused to exhibit, sensor and processes of the system to transmit [41, 42].

The altered or destructive elements should be eliminated from the pattern in the biometric system. During the preservation of quality for both duplication and distinct templates can be featured in mathematical form. In extraction a vowel of speaker is recorded depending on the vowels frequency of speech can be estimated in decision making. This data can be correlated with Algorithms and proceed for next feature extraction [43, 44]. It is an irreversible system i.e image cannot be extracted if once it is constructed. As per require bandwidth transmission initiated after feature extraction. Once in the data collection quality of system does not vary even though it is modified into good quality [45, 46].

The Template is to represent storage data, these features of the same type of a sample. The featured sample is Vector in mathematical notation [47-50], the stored template can also be known as Vector. The construction of template in data storage is Model producing features specific of a particular user. Models and features will be of different mathematical types and structures. Some models can be utilized to recognize voice and face [51-54]. Templates are prepared based on fingerprints, iris, and hand geometry recognition systems.

Enrollment is to place template or model into the database. Once in the database and coordinated with an unique identity by information externally, the biometric enrollment data is as the template or model for the pupil that it is referred. Generally many authentications can be carried by magnetic strip. To identify here the templates are matched calculating the distance in the pattern. In the model and sample of similar person, distances would be rare, be zero, if ever, as there would be always a non-duplicate biometric, result , sensor or transmission- that are related which vary remains after processing [55-64].

Data storage

The collection of registered templates is stored in Data storage. This stored data can been helpful for identification of the task given by the system [65]. It make easy to process to identify the data and generate output to recognize the task given by the system **(Figure 2)**.

Figure 2: Data collection to identify.

Collection of data in Biometric systems is a measure that depending on behavioral/physiological character [66-68]. It can be measured and used for distinctive individual and repeat several times. The troubles to measure and control this variation initiated at data collection subsystem.

User character should be designed for a sensor. The output of a biometric character in the sensor explains a behavior such as psychological component for all method in biometric system [69]. By the behavior components which might change in users, applications and test of the operation. Depending on the following character the output result can be generated.

The measurement of biometric input,

The method to generate output,

Technical conversion of the sensor.

Both duplicate and distinctive measure is negatively influence the change for any of this factor. Every system should maintain the unique standardized character to collect and represent the output. Collection of data should not coincide with data result in the given task. A proper management should be done to correlate with the previous records [70-75].

Matching algorithm

In the system templates are designed in such a pattern that can recognize the data and generate the output. This template can be matched depending on the minutes. Depending on the maximum minutes task can be completed to identify [76-78].

Decision process

This is the final component that gives the output result. After the matching is done depending on the minutes score the results can be made. If is the score is maximum then the result is yes and output is matched. If the score is low then the result is no and displayed as mismatch.

The decision process is implemented by the system from searching the database and analyze by "matches" or "mismatches". This is done on the basis of similarity (or) distance or either through measurements that are collected from the pattern match, and ultimately makes decision to either accept or reject decision depending on the system [79, 80]. As per the system, reject the identity claim of any individual's pattern is not acquired. Including the attained pattern, the program may confirm the match by a distance less than a fixed value and "accept" a user identity to claim can also depending on the single match or the program can declare a match of a distance lower than a user-dependent, time-variant, or environmentally linked required match in multiple measure for a decision to "accept". When the number is lower that can be made as false non-matches, against flying the number of false matches [81-83].

Uses of Biometric system

In many of government, businesses and organizations biometric system are used to analyze information regarding individual. These are improved because of security [85-89]. In airports device scan is done based on password such as bio-password to the system, or in data assemble procedure is an example of a biometric system that uses identifying data for a security result. In India Unique Identification Authority of India (UIDAI) has implemented Aadhar card for unique identification number for individuals. In figure 3 biometric systems used for data collection to generate Aadhar card [90-95].

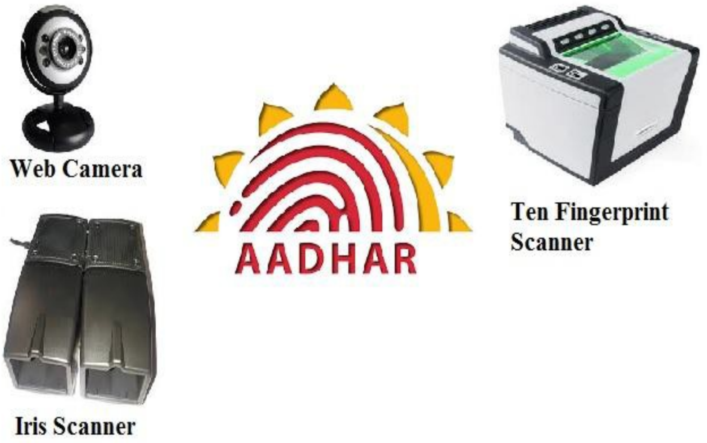

Figure 3: Biometric Systems used in Aadhar cards.

Biometric systems are utilized by the employees to register their attendance. Recently Indusland bank has implemented fingerprints as passwords for transaction. Hope there would be more advancement in the biometric system and useful for individuals [95-100].

REFERENCES

1. Rastogi P. Biometrics. Anthropology. 2015;2:e127.
2. Indrayani E. The Effectiveness and the Efficiency of the Use of Biometric Systems in Supporting National Database Based on Single ID Card Number (The Implementation of Electronik ID Card in Bandung). Journal of Information Technology & Software Engineering. 2014;4:129.
3. Prasathkumar V and Brindha E. Personal Authentication using Fingerprint Biometric System. International Journal of Innovative Research in Computer and Communication Engineering. 2014;2:1008-1014.
4. Kaushal N and Kaushal P. Human Identification and Fingerprints:A Review. Journal of Biometrics & Biostatistics. 2011;2:123.
5. Moghadam N, et al. A Robust Method for Fingerprint Recognition Using Biometric Fusion. Journal of Biometrics & Biostatistics. 2012;3:143.
6. Warade S and Patil R. Touch-less Fingerprint Recognition Using SVM and GMM:A Comparative Study. International Journal of Innovative Research in Computer and Communication Engineering. 2015;3:4053-4059.
7. Spaun NA. Forensic Biometrics from Images and Video at the Federal Bureau of Investigation. Biometrics: Theory, Applications, and Systems. 2007;1-3.
8. Naveed G and Batool R. Biometric Authentication in Cloud Computing. Journal of Biometrics & Biostatistics. 2015;6:258.
9. Kamble P and Nikumbh S. Security System in ATM using Multimodal Biometric System and Steganographic Technique.International Journal of Innovative Research in Computer and Communication Engineering. 2015;4:2161-2167.
10. Riera A, Soria-Frisch A, et al. Unobtrusive Biometric System Based on Electroencephalogram Analysis. EURASIP Journal on Advances in Signal Processing. 2007;2008:1-8.
11. Cross JM and Smith CL. Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification. Security Technology. 1995;20-35.
12. Uludag U, et al. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE. 2004;92: 948-960.
13. Zhang DD. Human Body and Biometrics. Automated Biometrics: Technologies and Systems. 2000;7: 23-42.
14. Logeshwari R, et al. Designing a Bio-Capsule Secure Authentication System. Journal of Information Technology & Software Engineering. 2015;5:138.
15. Prabhakar S, et al. Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy. 2003;99:33-42.
16. Jain AK, et al. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004;14:4-20.
17. Zhou X, et al. A master-slave system to acquire biometric imagery of humans at distance. ACM SIGMM international workshop on Video surveillance. 2003;113-120.
18. Ghosh P and Dutta R. A new approach towards Biometric Authentication System in Palm Vein Domain. International Journal of Advance Innovations, Thoughts & Ideas. 2012;1:1-10.
19. Vijay Kumar N and Sivasubramanyam M. A New Pairing Method for Latent and Rolled Finger Prints Matching. International Journal of Innovative Research in Computer and Communication Engineering. 2014;2:5277-5283.
20. Banerjee HN, et al. Deciphering the Finger Prints of Brain Cancer Glioblastoma Multiforme from Four Different Patients by Using Near Infrared Raman Spectroscopy. Journal of Cancer Science & Therapy. 2015;7:044-047.
21. Al-Hamdani O, et al. Multimodal Biometrics Based on Identification and Verification System. Journal of Biometrics & Biostatistics. 2013;4:163.
22. Kanchan T and Krishan K. Personal Identification in Forensic Examinations. Anthropology 2013;2:114.
23. Ross A and Jain A. Information fusion in biometrics. Pattern Recognition Letters. 2003;24:2115–2125.

24. Kukula EP and Proctor EW. Human-Biometric Sensor Interaction: Impact of Training on Biometric System and User Performance. Human Interface and the Management of Information. Information and Interaction. 2009;5618:168-177.
25. Ross A and Jain A. Biometric Sensor Interoperability: A Case Study in Fingerprints. Biometric Authentication. 2004;3087:134-145.
26. Fang R, et al. STR Profiling of Human Cell Lines:Challenges and Possible Solutions to the Growing Problem. Journal of Forensic Research. 2011;S2:005.
27. Nwankwo N. Digital Signal Processing Techniques:Calculating Biological Functionalities. Journal of Proteomics & Bioinformatics. 2011;4:260-268.
28. Papp Z. Demon Chip - Polarised Biometrics Based on DSP and RFID. Journal of Forensic Research. 2015;6:306.
29. Morshed B and Khan A. A Brief Review of Brain Signal Monitoring Technologies for BCI Applications:Challenges and Prospects. Journal of Bioengineering & Biomedical Science. 2014;4:128.
30. Lim S, et al. Efficient Iris Recognition through Improvement of Feature Vector and Classifier. ETRI Journal. 2001;23: 61-70.
31. Vatsa M, et al. Comparison of iris Recognition Algorithms. Intelligent Sensing and Information. 2004;354-358.
32. http://www.omicsonline.org/scholarly/digital-signal-processing-journals-articles-ppts-list.php
33. Soutar C, et al. Biometric Encryption using image processing. Optical Security and Counterfeit Deterrence Techniques II. 1998;3314:178.
34. Senthilkumar S. Impact of Signal and Image Processing, Communications and Networking. Journal of Electrical & Electronic Systems. 2014;3:e114.
35. Chandanapalli SB, et al. Design and Deployment of Aqua Monitoring System Using Wireless Sensor Networks and IARKick. Journal of Aquaculture Research & Development. 2014;5:283.
36. Kreymer E. Guarcs in the Inside Hadronic Four-Dimensional Euclidean Space with Real Time. Journal of Physical Mathematics. 2015;6:140.
37. Abbas U, et al. Design and Implementation of Advanced Wireless Tongue Drive/Operated System for Paralyzed, Disabled & Quadriplegic Patients. Journal of Bioengineering & Biomedical Science. 2016;6:185.
38. Srivastava JB, et al. Implementation of Digital Signal Processing Algorithm in General Purpose Graphics Processing Unit(GPGPU). International Journal of Innovative Research in Computer and Communication Engineering. 2013;1:1006-1012.
39. Garcha SS and Kaur H. A Robust Technique Implementation for Facial Recognition under Eigen Feature Extraction. JGRCS 2013;4:18-20.
40. Srivastava SK and Abdulhalim I. Spectral Interrogation based SPR Sensor for blood Glucose Detection with Improved Sensitivity and Stability. Journal of Biosensors & Bioelectronics. 2015;6:172.
41. Barizuddin S, et al. Plasmonic Sensors for Disease Detection - A Review. Journal of Nanomedicine & Nanotechnology. 2016;7:373.
42. Kaushika A, et al. Miniaturized Sensing Devices for Biomarker Detection. Journal of Biosensors & Bioelectronics. 2015;6:e132.
43. Sul S. Classification-based Automatic Fingerprint Identification System for Large Distributed Fingerprint Database. Journal of Biometrics & Biostatistics. 2011;2:111.
44. Lissner J. Theory for Determining Energy Value in Nanometric Biophysical Systems. Journal of Astrobiology & Outreach. 2015;3:141.
45. Celik N, et al. Multimodal Biometrics for Robust Fusion Systems using Logic Gates. Journal of Biometrics & Biostatistics. 2015;6:218.
46. Al-Hudhud G. The synergy of biometrics and adaptive technologies for smart world. Journal of Applied & Computational Mathematics. 2015;4:5.
47. http://research.omicsgroup.org/index.php/Vector_notation
48. Namio FT, et al. Mathematical Model of Complete Shallow Water Problem with Source Terms, Stability Analysis of Lax-Wendroff Scheme. Journal of Theoretical and Computational Science. 2015;2:132.
49. Bakach I and Braselton J. A Survey of Mathematical Models of Dengue Fever. Journal of Computer Science & Systems Biology. 2015;8:255-267.
50. Szczesniak RD, et al. Mixtures of Self-Modelling Regressions. Journal of Biometrics & Biostatistics. 2014;S12:003.

51. Brindha VE. Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. Journal of Biometrics & Biostatistics. 2012;3:145.
52. Verma D and Dubey S. A Survey on Biometric Authentication Techniques Using Palm Vein Feature. JGRCS 2014;5:5-8.
53. Supriya VG and Manjunatha R. Chaotic Maps for Biometric Template Protection-A Proposal. Journal of Biometrics & Biostatistics. 2015;6:216.
54. http://research.omicsgroup.org/index.php/Prosopagnosia
55. Brindha VE. Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. Journal of Biometrics & Biostatistics. 2012;3:145.
56. Chen CK, et al. Data Encryption and Transmission Based on Personal ECG Signals. International Journal of Sensor Networks and Data Communications. 2015;4:124.
57. Rautaray J and Kumar R. Privacy Preserving in Distributed Database Using Data Encryption Standard (Des). International Journal of Innovative Research in Science, Engineering and Technology. 2013;2:566-571.
58. Singh HP, et al. Secure-International Data Encryption Algorithm. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2013;2:780-792.
59. Chabbra S and Singh N. Applications of Swarm Intelligence in Biometrics systems. International Journal of Innovative Research in Computer and Communication Engineering. 2:3089-3094.
60. Basu S. International Data Encryption Algorithm (Idea) - A Typical Illustration. JGRCS 2011;2-116-118.
61. Krishna AVN. Study of the Effects of Noise on a New Model Based Encryption Mechanism with Time-Stamp and Acknowledgement Support in MANET & WSN Environment. International Journal of Advancements in Technology. 2011;2:14-21.
62. Krishna AVN. Probabilistic Encryption Based ECC Mechanism. IJICT 2011;2:257-268.
63. Taneja S, et al. Encryption Scheme for Secure Routing in Ad Hoc Networks. IJICT 2:22-29.
64. Akilan P, et al. Design of Two Tier Security ATM System with Multimodal Biometrics By Means of Fuzzy Logic. International Journal of Innovative Research in Science, Engineering and Technology. 2014;3:1283-1288.
65. http://research.omicsgroup.org/index.php/Encryption
66. Janiak M, et al. Biometric authentication device for use with token fingerprint data storage. 2002;US 20020097142 A1.
67. Harris JM, et al. Personal data storage and transaction device system and method. 2001;US 6331972 B1.
68. Karthik R and Chowdhury PKR. A comparison of data storage technologies for remote sensing cyber-infrastructures. J Data Mining In Genomics & Proteomics 2015;6:4.
69. Chiba Y, et al. On the Identification of the Survivor Average Causal Effect. Journal of Biometrics & Biostatistics. 2011;2:e104.
70. Escabias M, et al. Functional Data Analysis in Biometrics and Biostatistics. Journal of Biometrics & Biostatistics. 2012;3:e120.
71. Jassim SA. Face recognition in uncontrolled conditions - Can compressive sensing and super-resolution meet requirements of this challenge? Journal of Biometrics & Biostatistics. 2013;4:4.
72. Choi D. Biosensors and Bioelectronics. International Journal of Sensor Networks and Data Communications. 2016;S1:e002.
73. Atkinson KF and Nauli SM. pH sensors and ion Transporters:Potential therapeutic targets for acid-base disorders. International Journal of Pharma Research & Review 2016;5:51-58.
74. Das AP. Biosensors:The Future of Diagnostics. International Journal of Sensor Networks and Data Communications. 2016;S1:e107.
75. Hu JJ, et al. Blocking Non-Specific Binding for Phage-Based Magnetoelastic Biosensors. Biosensors Journal. 2015;4:130.
76. Othman M, et al. Modelling of Dynamic Response of WO3 Gas Sensors under CO. RRJSMS 2015;1:40-46.
77. Basha SK and Vasavi G. KareemNaaz-Vasavi (KV) Pattern Matching Algorithm. Research & Reviews: Journal of Engineering and Technology 2015;4:22-24.
78. Anbarasan M and latha k. Resistance Matching Algorithm for MPPT of Fuel Cell System. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2014;3:32-40.
79. Divakar S and Satyanarayana RVS. Comparison of Matching Algorithms for MST Radar Data. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2013;6271-6278.

80. 64. Wolff A. Lab-on-a-chip system with integrated sensors for 3D tissue engineering applications. Biological Systems:Open Access. 2015;4:2.
81. Tobolova M, et al. Testing the Effects of Micro-Pulse Stimulation on Blood Circulation Using the Thermodynamic Sensors. Journal of Biosensors & Bioelectronics. 2014;5:147.
82. Nithya M. Electrochemical Sensing of Ascorbic Acid on ZnO-decorated Reduced Graphene Oxide Electrode. Journal of Biosensors & Bioelectronics. 2015;6:164.
83. http://research.omicsgroup.org/index.php/Sensor-based_sorting
84. Inoue S and Ishida Y. Design of a Model-following Controller Using a Decoupling Active Disturbance Rejection Control Method. Journal of Electrical & Electronic Systems. 2016;5:174.
85. Kihal N, et al. A new biometric database based on corneal topography. Journal of Applied & Computational Mathematics. 2015;4:5.
86. Sul S. Classification-based Automatic Fingerprint Identification System for Large Distributed Fingerprint Database. Journal of Biometrics & Biostatistics. 2011;2:111.
87. Meanon N and Krishnamurthy R. Forensic analysis of digital fingerprint based biometric data. Journal of Forensic Research. 2014;5:6.
88. Fernández RS. Fingerprint template protection scheme, security and vulnerabilities:A survey. Journal of Biometrics & Biostatistics. 2014;5:4
89. Lee SY, et al. Microbial Forensic Analysis of Bacterial Fingerprint by Sequence Comparison of 16S rRNA Gene. Journal of Forensic Research. 2015;6:297.
90. http://research.omicsgroup.org/index.php/Video_remote_interpreting
91. http://research.omicsgroup.org/index.php/Iris_recognition
92. Gawande U, et al. Improving Iris Recognition Accuracy by Score Based Fusion Method. International Journal of Advancements in Technology. 2010;1:1-12.
93. Jaiswal Y and Dewangan SK. Study and Analysis of Indigenous Risk Impact Screen (Iris) in Alcohol Presence Using Textural Features. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2013;2:1002-1005.
94. http://research.omicsgroup.org/index.php/Unique_Identification_Authority_of_India
95. Chavali A and Nalini C. Observing the Effects of Colored Lenses on Iris Recognition using Feature Extraction Technique. International Journal of Innovative Research in Science, Engineering and Technology. 4:1734-1740.
96. Bhatti B. Aadhaar-Enabled Payments for NREGA Workers. Economic & Political. 2012;48: 16-19.
97. Dhongde VS, et al. IRIS Recognition Using Neural Network. International Journal of Innovative Research in Science, Engineering and Technology. 2014;3:471-482.
98. Kataria AN, et al. A survey of automated biometric authentication techniques. Nirma University International Conference on Engineering. 2013;1-6.
99. Brindha VE and Natarajan AM. Multi-Modal Biometric Template Security:Fingerprint and Palmprint Based Fuzzy Vault. Journal of Biometrics & Biostatistics. 2012;3:150.
100. Pandey AB, et al. Empowering India through unique IDs to 1.2 billion Indians. Journal of Biometrics & Biostatistics. 2013;4:4.