International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Transforming Voters Registration Paradigm in Tanzania, The Shift from OMR to BVR

Dennis N Mwighusa

[1]St Joseph University, School of Electrical and Electronics Engineering, P.O.Box 11007, Dar es Salaam, Tanzania

Abstract: ***Voter registration is very important towards election processes especially in most of developing countries such as Tanzania. Electioneering process normally leads to election fraud such as double registration and other forms of election drawbacks during registration of voters and casting of votes by eligible voters. For the election to be fair in both contesting parties and accurate then needs to have a known number of voters eligible to cast their votes. The electoral roll is usually constructed by means of a voter registration system that compiles voter's data. In the past ended Tanzanian elections, Optical Mark Recognition registration and verification system was introduced during the registration and verification of voters. It was observed on the elections day that some of the genuine registered voters were not recognized by the electoral officers hence they were disfranchised from voting which is against the constitutional rights of every Tanzanian who had reached the age of eighteen at the time of the registration of voters. This was caused due to various problems like a voter to have moved in a different place from where he/she registered and many others. The current system for voter registration has got many deficiencies such as lack of effective methods to prevent impersonation, multiple registrations and alterations on voter information. In this paper the proposed system for voter registration increases the accuracy of the current systems. Here the registration is carried out by means of biometric voter registration (BVR). Biometric Voter Registration is used to prevent impersonation, detect multiple registrations from the same person and protect from alterations the registration information. This system will also help before a voter could be allowed to cast his / her vote the biometric machine will be supposed to recognize him/her first. This paper uses a multi scan system that allows citizens to use different parts of their bodies to go through the registration and verification process, here we shall observe the use of both fingerprint, facial and signature types of recognition techniques. The introduction of this proposed system for general elections is expected to create room for full participation of all eligible voters, eliminate multiple voting and also increase the confidence of the people in Tanzania in the electioneering process.***

Keywords: Biometric, BVR, Registration, Fingerprint, OMR

1. Introduction

Voter Registration allow the populace to choose their representatives and express their preferences for how they would be governed. The integrity of registration process is fundamental to the integrity of democracy itself.

Lately, there has been an increasing interest to improve the efficiency in the registration hence voting processes, which has resulted in a wide range of proposals for new election systems. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage.

Voter registration is the process to collect the voters' data in order to constitute an electoral roll. Because of the fact that the electoral roll determine if a voter has the right to cast a vote during the voting stage, it has to be formed in an efficient way. Even when voting and tallying stages have the greatest security level, a deficient voter registration system can facilitate fraud practices that can even affect the accuracy of the election.

Voter registration is conventionally carried out face to face with the registration authority. As in Tanzania the Current voter registration systems OMR – Optical Mark Recognition have important issues that can facilitate voter impersonation. These issues are mainly voter identification accuracy, multiple registrations from the same person and voter registration information integrity. In this paper we proposed the use of biometric voter registration system to encounter the above measures. The use of both Fingerprints, Facial and Signature technologies have been used simultaneously. The accuracy of biometric devices depends on human, device, and algorithm factors. Each can provide very accurate assessments, but if any one of them has problems, then this can compromise the accuracy of the biometric device.

Figure 1: Voter ID Card with OMR Technology

In this paper we propose a Biometric Voter Registration system, in which some biometric systems play an important roll to protect the accuracy of the electoral roll. The new technology will help to address the challenges such as double registration, identify voters during elections and transfer voter information from one place to another especially when a person has shifted from where he/she was once registered. However, in the context of this paper, voter registration is related to the creation of the electoral roll.

Figure 2: Proposed BVR IDCard(Hologram)

2. Optical Mark Recognition (OMR) / Existing System

The permanent voters' register was introduced in 2004 with the use of the Optical Mark Recognition which involved the use of Polaroid camera.

At the time, the biological data included passport size photos and signatures. Thumb prints were added when a digital registration kit was used during its updating in 2009. For the second time the book was updated in 2009/2010 to register new eligible voters for the 2010 general election.

The old method of registering voters did not have an in-built mechanism for detecting multiple registrations and therefore, there were instances where some unscrupulous individuals registered more than once.

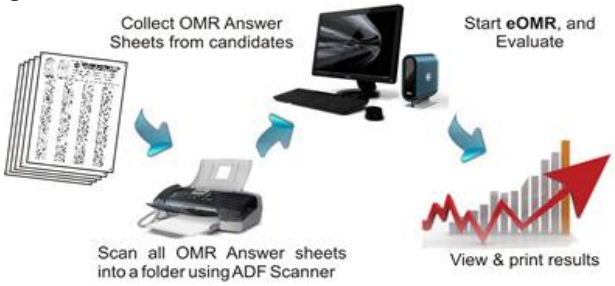

Figure 3: The OMR system how it works

Often with this technology there was no reliable register beforehand or the identification documents have been of such standard that falsification has been easy. A common occurrence is that the registration process has not been designed to easily allow for a change of address, wherefore people when moving re-register without having their old record deleted. Past conflicts including votes by minors and the dead, in addition to missing voters who were actually eligible to vote pushed the commission to implement biometric voter registration. The technology will not be used during the actual voting process.

3. Biometrics

Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioral characteristic of the user. Biometrics systems are classified based on the unique characteristic of the user that is used for the identification, for instance: DNA, face, fingerprint, iris, palmprint, retina, writing/signature and voice. However, the accuracy on the different biometric system is not the same, since each of the biometric characteristics processed has advantages and disadvantages.

A good biometric characteristic must fulfill some requirements:

- Performance; It refers to the speed and accuracy of recognition as well as the resources required to do it (cost).
- Robustness; It reflects the level of resistance against fraudulent methods attempting to mislead.
- Acceptability; It indicates the level of acceptance of people to use the characteristic.
- Uniqueness; It is how well the characteristic makes different two individuals.
- Permanence; It is how well the characteristic endure over the time.
- Universality; Each individual should have the characteristic.
- Collectability; Ease to acquire the characteristic.

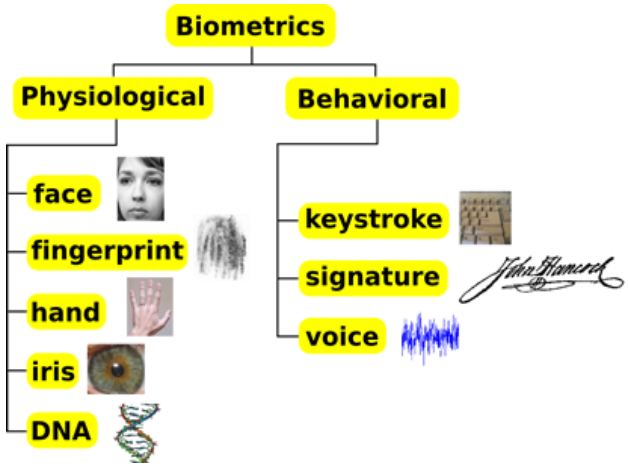

Figure 4: Types of Biometrics technologies

4. Biometric Voter Registration (BVR)

This is a Voter Registration System for automatic data capturing with advanced OMR and direct capturing of biometric fingerprints, facial picture and digital or digitized signature for verification and de-duplication. It can also be defined as the use of computers, fingerprint scanners and digital cameras to capture the bio-data of applicants. Fingerprints are unique to every individual and it is these unique features and other details that will be stored in the computer from which the voters register is produced. The BVR is a highly advanced information system that enrols and identifies millions of voters quickly and distinctly. With biometric identifiers, the possibility of election fraud is minimised and the voter identification process is also accelerated considerably. With biometric technology, the detection and removal of multiple registrations from the system will be made possible with relative ease thus, a more accurate and reliable register will be produced.

The BVR system uses a computer finger-print scanners and digital cameras to capture the bio-data of an applicant. The personal details of finger-prints and face photo technology are used to verify the authenticity of the voter, and to ensure greater transparency and credibility in the elections.

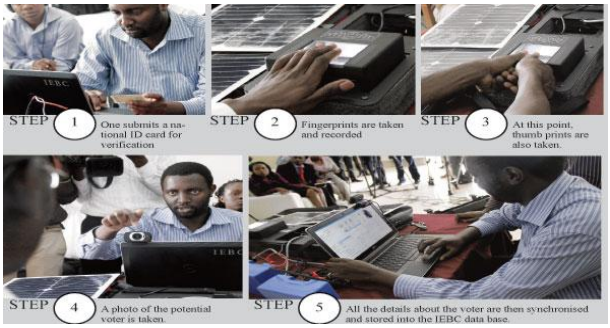

Figure 5: Steps taken for Biometric Voter Registration

4.1. BVR Kit

The field registration kits includes:
Hardware:

- Fingerprint scanner/reader for capturing fingerprint images for each voter registered, webcam for capturing facial images for each voter registered, notebook computer for processing of enrollment data, printer for issuance of voter ID cards, data storage and backup (USB thumb drives), microsoft windows operating system, electronic power supply board.

The back-end system includes:

- Multi-biometric technology software for analysis of the biometric data, MySQL for the voter registry database and other related softwares, all necessary software.

The power unit comprises:

- An external power supply (choice of lead battery, solar panel or lithium-ion battery), all necessary cables including a security cable and lock for the generator, a battery charger and tester used to charge and test the battery

Figure 6: BVR Kits

Each unit provides an 12-hour power supply to the mobile enrolment unit in areas where there is no power, such as isolated villages. Also the solar panels when they are used can retain an extra charge for more 4 hours.

The BVR system has the GPS and 3G internet for direct link with the main Database upon sending the registration details on the spot. Where network connectivity is absent, a USB thumb drive is a highly effective and secure means of transferring encrypted data from field units to the regional and national levels.

To protect the equipment during transport and storage, field registration units are housed inside dust/water-proof and shock resistant cases. The interior of the case is fitted with a custom designed foam insert to secure the electronic components for safety during transport and storage. Equipment is removed from the kit following arrival at a registration center; a foolproof process that requires just several minutes as only standard USB connections are used.

4.2. Quality of the ID card

Once the registration is completed and de-duplication performed, an important anti-fraud measures is the ID card. If the ID card is easy to forge then identity theft or impersonation can be easy. A photo ID with significant security features such as **holograms** refer to *figure 2* above, microprint and invisible print will make it significantly harder to vote on behalf of someone else.

5. Proposed System/ Registration

5.1 Operation

Voter's details that will be captured including names, age, gender, finger prints, and a face photograph. Other details captured includes voters registration centre name, polling station name, Assembly ward name, Constituency and County name. Fingerprints, Facial images, and the underlying biometric data of each registrant are captured at the time of registration. Built-in quality parameters ensure these templates are suitable for matching purposes, enhancing the quality and speed of that operation. The biometric data is stored as part of the voter record and is fully encrypted along with personal information to ensure security and privacy policies are respected.The all registration process of an individual takes only 3 minutes. Printing the card is done for 15 to 17 seconds through the PVC card printer.

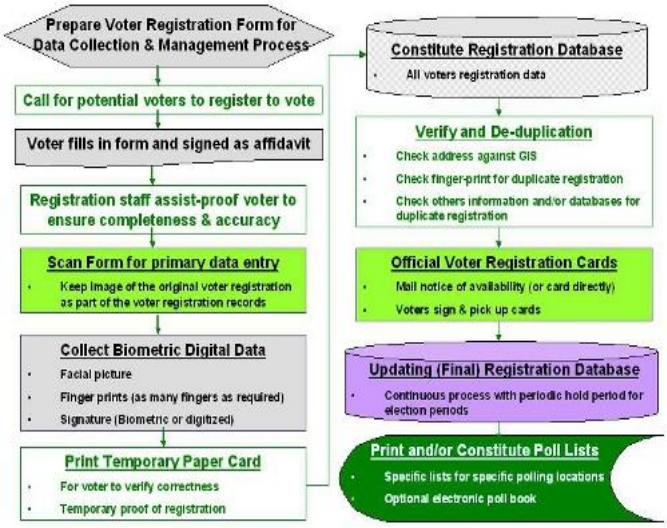

Figure 7: BVR Registration System

5.2 Biometric Fingerprint

Human fingerprints are unique to each person and can be regarded as a sort of signature, certifying the person's identity. A fingerprint is formed from an impression of pattern of ridges on a finger. A ridge is defined as a single curved segment and a valley is the region between two adjacent ridges. The minutiae which are the local discontinuities in the ridge flow pattern provide the features that are used for identification. Current trend is to capture

four prints: thumbs and index fingers of both hands. As for fingerprinting it is highly advisable that the registration computer has software that can determine on the spot whether a suitable template can be developed.

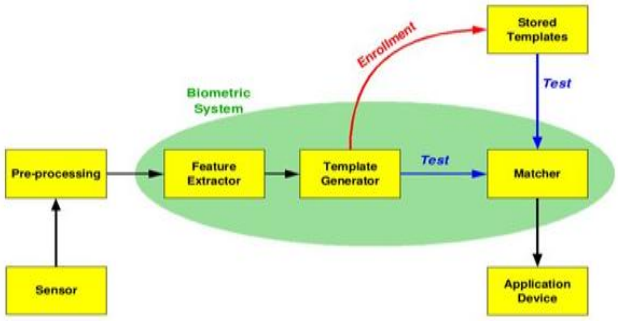

Figure 8: Biometric System Diagram

5.2.1.How to Read a Fingerprint

There are three ways to read fingerprints: By pattern types, by the size of the patterns, and by their position on the fingers. There is a science to this called dactyloscopy, which is the practice of identifying someone using fingerprints. The method to identify fingerprints starts from the thumb to the little finger for each hand, then as a group with the four fingers held closer together and the thumbs printed again, individually, for each hand.

5.2.2.Accuracy of Fingerprint Biometrics

There are at least three factors that you must take into account to make the biometric accurate.

5.2.2.a.Human Factor

For fingerprint capture, several elements must be in place. Fingers must be in contact with a sensor surface.

5.2.2.b.Device Factors

The technology of biometric sensors also can be a source of errors notwithstanding adequate capture procedures. Environmental conditions and technological properties of devices affect the quality of the captured biometric records.

5.2.2.c.Algorithm Factor

A biometric algorithm has three components - enrolling, evaluation, and decision-making. **Enrolling** analyzes the biometric data, extracts its features, and puts them into a compact biometrical template structure. **Evaluation** assigns a similarity score to the comparison between two templates. The first compared record is a query template and the second one the candidate template. If the two record comparisons belong to the same person this is a genuine comparison. If not, it is an impostor comparison. **The decision-making** component uses the score as determined by a matching or ranking algorithm to make a decision about the comparison between two templates. The matching algorithm determines if the comparison is genuine or not. On the other hand, the ranking algorithm uses a predefined integer value to compare the result to the stored database of individuals. It finds the most common templates that match the query template.

6. Conclusion

Although this system provides best solutions to problems related to the Tanzanian voter registration system but it is still vulnerable to security attacks. Confidential biometric data may be leaked due to network connectivity or system hacking. Registration information collected in other countries included same BVR technology. However, the reports describes that problems arose during registration, procedures and technical controls were not strong enough to prevent the problems associated with, and the fingerprint and photograph data were not good enough to allow the duplicates to be detected at the centre. and hence this problem need to be resolved if the same happens to Tanzania. It is in this context that we will have to consider of a far more accurate, efficient and precise technology of iris recognition for voter registration. Iris recognition is considered as a possible more powerful means of de-duplication of the voting register for the elections.

References

[1] Cappelli, R. et. al.: "Performance evaluation of fingerprint verification systems," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, January 2006.
[2] KoichiroNiinuma, Unsang Park and Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 771-780, Dec. 2010.
[3] Anil K. Jain, Patrick Flynn and Arun A. Ross, "Handbook of Biometrics," Springer Science, ISBN-13: 978-0-387-71040-2, 2008.
[4] Krivoruchko, T,"Robust Coercion-Resistant Registration for Remote E-voting", Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.
[5] Electoral Services International Inc.,"An Introduction to ESI Inc.'s highly successful multi-biometric voter registration solution", www. esi-sei.com.
[6] Kevin W. Bowyer, Estefan Ortiz, and Amanda Sgroi, "Trial Somaliland Voting Register", De - Duplication Using Iris Recognition, Department of Computer Science & Engineering, University of Notre Dame, Notre Dame, IN 46566 USA.
[7] Saurabh Yadav, Ajay Kr. Singh, "A Biometric Traits based Authentication System for Indian Voting System", International Journal of Computer Applications, Volume 65 – No.15, March 2013.
[8] How to Read a Finger Print, Image http://en.wikipedia.org/wiki/File:Fingerprint_picture.svg .
[9] Accuracy of Finger Print Biometrics Image:http://commons.wikimedia.org/wiki/File:Biometric_system_diagram.
[10] Thomas Yeboah, Edward Opoku-Mensah, Christopher AyaabaAbilimi, "A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission", Journal of Engineering, Computers & Applied Sciences (JEC&AS), Volume 2, No.7, July 2013.

[11] Dimitris A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, Vol. 21, No 6, pp. 539-556, 2002.
[12] Electoral Commission' website to register to vote. Available online at http://www.aboutmyvote.co.uk/register/CitzSelect.cfm?officeID=214&CFID=12799012&CFTOKEN=71181288.
[13] NeurotechnologyVeriEye SDK, http://www.neurotechnology.com/verieye.html
[14] Nathan David, DaberechiUbachukwu, Hyacinth Ijomanta, Chukwuebuka Gil-Ozoudeh, "A Biometric based Software Solution for E-Voting using networking", Scholars Journal of Engineering and Technology (SJET), Sch. J. Eng. Tech., 2014; 2(6B):874-881.

Author Profile

Eng. Dennis Mwighusaholds Bachelor and Master of Engineering in both Computer Engineering and Science and Electronic Engineering (Signal and Information Processing) from St Joseph University in Tanzania and Tianjin University of Technology and Education in Tianjin, P. R. He is also a Registered Professional Engineer (PEng) with Engineers Registration Board (ERB) - Tanzania, a member of Institute of Electrical and Electronics Engineers (IEEE), Asia Pacific Signal and Information Processing Association (APSIPA) and Institute of Engineers Tanzania (IET). Currently working as Managing Partner of DEN CONSULT LIMITED, Assistant Lecturer – (SJUIT), and Research Assistant. His research interest includes Signal and Image Processing, Pattern Recognition, Computer Vision, Neural Networks and Wavelet Analysis.