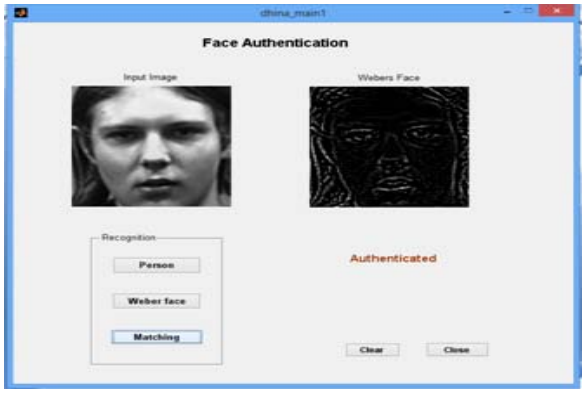

Figure 6: Matching

7.2. Fingerprint Verification

The input fingerprints are taken using the fingerprint scanner. Here, system takes two fingerprints images to be matched and gives the percentage score of matching between them. Based on the percentage score and the threshold value, it can distinguish whether the two fingerprint match or not The fingerprint verification is simulated in visual basic 6.0. Initially, the fingerprint image is captured using the fingerprint scanner and it is saved. In this way, various fingerprint templates can be created and saved. Once, the fingerprint image is ready for verification, it is verified for various inputs to display whether the person is authenticated or not. The snapshots for fingerprint verification are shown below:

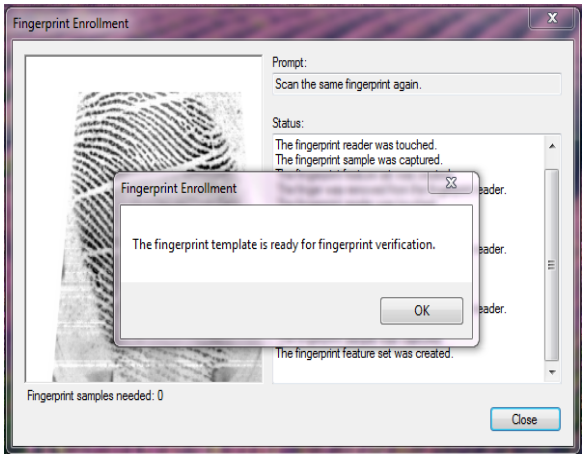

Figure 7: Fingerprint Enrollment

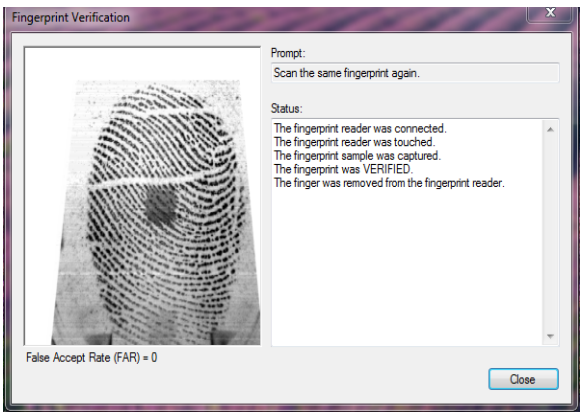

Figure 8: Fingerprint Verification

8. Conclusion and Future Work

A bimodal security system is implemented which includes the finger print and face recognition system in order to provide secure voting process. The GSM modem is also used to enable automatic counting of votes and it also makes the counting process faster. We are implementing the face recognition and fingerprint verification in the ARM7 microcontroller. The input image will be captured using the webcam and it will be verified automatically. LCD is interfaced to the output port of the microcontroller and it is used to show the information regarding the voting options available to the voters. GSM modem is interfaced to the microcontroller for the automatic counting of the votes. The software coding is dumped into the microcontroller using the keil c and the circuit is designed in ORCAD.

References

[1] Vaibhav Bhatia, Rahul Gupta (2014), "A Novel Electronic Voting Machine Design with Voter Information Facility Using Microcontroller", International Conference on Computing for Sustainable Global Development (INDIACom).
[2] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi (2011), "Online Voting System Powered By Biometric Security Using Steganography", Second International Conference on Emerging Applications of Information Technology.
[3] Hyejeong Lee, Sang-Ho Lee, Taeseok Kim, and Hyokyung Bahn (2008),"Secure User Identification for Consumer Electronics Devices", IEEE Transactions on Consumer Electronics, Vol. 54, No. 4.
[4] David Molnar, Tadayoshi Kohno, San Diego, Naveen Sastry David Wagner (2006),"Tamper-Evident, History Independent, Subliminal-Free Data Structures on PROM Storage", Proc.IEEE Symposium on Security and Privacy.
[5] Barbara Ondrisek (2009), "E-Voting System Security Optimization," Proceedings of the 42nd Hawaii International Conference on System Sciences.
[6] Ng Su Gnee (2009), "A Study of Hand Vein, Neck Vein and Arm Vein Extraction for Authentication," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4.
[7] M. Bishop, and D. Wagner (2007), "Risks of e-voting," Communications of the ACM, Volume 50, Issue 11. COLUMN: Inside risks. ACM, p. 120.
[8] Yun-he Li, Shan-yu Wu (2008), "Research on a New E-voting Method based on the Cellular Phone Electronic Commerce and Security," 2008 International Symposium on Guangzhou City, pp. 318-321, 3-5.
[9] Azgomi, M.A., Makoo Branch (2009), "An architecture for e-voting systems based on dependable web services," Innovations in Information Technology, IIT International Conference on Al Ain, pp.200 – 204, 15-17.