Figure 7. Partial compromising of transformation keys of random projection Y= OX+b where 10%, 20%,.., 100% of the transformation key is guessed. A) Equal Error Rates (EER %) in two setups: b is zeor vector, and b is non-zeor vector, B) False Acceptance Rates(FARs) and False Rejection Rates(FRRs) of two-factor face authentication where b is a zero vector , and C) FARs and FRRs of two-factor face authentication where b is a non-zero vector.

7. References

[1] A. Adler, Vulnerabilities in biometric encryption systems. 2005. Proc. of Audio and Video-Based Biometric Authentication. Vol. 3546, pp. 1611-3349.

[2] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. 2007. Fingerprint Image Reconstruction from Standard Templates. Pattern Analysis and Machine Intelligence. Vol. 29(7), pp. 1489-1503.

[3] A. Teoh, D. Ngo, A. Goh. BioHashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition. Vol. 37(11), pp. 2245-2255, 2004.

[4] L. Alessandra and L. Nanni, "Empirical tests on BioHashing", Neurocomputing, pp. 2390-2395, 2006.

[5] Anil K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing. pp. 1-17, 2008.

[6] Andrew B. J. Teoh, Kar-Ann Toh, and WK. Yip, "2^N Discretisation of BioPhasor in Cancellable Biometrics. Advances in Biometrics", pp. 435-444, 2007.

[7] A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for dual-factor authentication", Pattern Analysis & Applications. Vol. 7(3), pp. 255-268, 2004.

[8] Y. Wang and K. Plataniotis, "Face based biometric authentication with changeable and privacy preservable templates", Biometrics Symposium, pp. 1-6, 2007.

[9] A. Konga, K. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants. Pattern Recognition", Vol. 39, pp. 1359-1368, 2006.

[10] A. Konga, K. Cheung, D. Zhang, M. Kamel, J. You., "Revealing the Secret of FaceHashing", Advances in Biometrics, pp. 106-112, 2006.

[11] Christian Rathgeb and Andreas Uhl, "Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems", Proc. of the 7th International Conference of Image Analysis and Recognition (ICIAR-2010), pp.296-305, 2010.

[12] Y C Feng, Pong C Yuen and Anil K Jain, "A Hybrid Approach for Face Template Protection", Proc. SPIE, Vol. 6944, p.p. 694408, 2008.

[13] H. Al-Assam, H. Sellahewa, and S.A. Jassim, "Lightweight approach for biometric template protection", Proc. SPIE. Vol. 7351, p.p. 73510, 2009.

[14] S. Kanade, D. Camara, B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris", Biometrics Symposium, pp. 59-64, 2008.

[15] H. Al-Assam, H. Sellahewa, and S.A. Jassim, "Multi-factor biometrics for authentication: a false sense of security", Proc. of the 12th ACM workshop on Multimedia and security, p.p. 81-88, 2010.

[16] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti., "Filterbank-Based Fingerprint Matching", IEEE Trans. Image Processing. Vol. 9(5), pp. 846-859, 2000.

[17] D Maltoni, D Maio, AK Jain, S Prabhakar, "Handbook of fingerprint recognitionun 2ed Edition", 2009.

[18] Harter, F.S. Samaria, "Parameterisation of a stochastic model for human face identification", Proc. 2nd IEEE workshop Applications of Computer Vision, 1994.

[19] Chinese Academy of Sciences. Institute of Automation CASIA Iris Image Database: http://www.cbsr.ia.ac.cn. (Access date: 6 May 2009)

[20] S Jassim, H Al-Assam, H Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques", Image and Signal Processing and Analysis, pp. 556 – 561, 2009.

[21] J. Daugman, "How iris recognition works". Proc. of Int. Conference on Image Processing, Vol. 1, 2002.