**ABSTRACT**

Biometric scheme are being widely employed because their security merits over the earlier authentication system based on records that can be easily lost, guessed or forged. High scale employments and the related template storage have increased the requirement to guard the biometric data stored in the system. Theft of biometric information is a negotiation of the user’s privacy. In Addition, the stolen biometric information can be used to access other biometric systems that have the similar feature provided for the user. Several alternative functions have been identified in literature for creating revocable or noninvertible biometric templates. Although, their security examination either disregards the distribution of biometric features or uses inefficient feature matching. This generally shows the way to unrealistic approximation of security. In this paper a novel approach for the Non-Invertible biometric system is proposed to secure the biometric template. Security of a feature transformation method can be assessed according to the two main factors: i) non-invertibility, and ii) diversity. Non-invertibility represents the complexity in obtaining the original biometric when the secure template is provided and diversity represents the complexity in guessing one secure template when a different secure template created from the identical biometric is provided. The proposed Non-invertible Gabor transform possess both the non-invertible and diversity features which enhances the security of the system to a large extent. The proposed approach is very much resistant to minor translation error and rotation distortion. The experimental result shows the better performance of the proposed technique compared to the existing system