Visual Cryptographic Schemes using Combinatorial Designs; their Construction and Optimality

Mausumi Bose
Applied Statistics Unit
Indian Statistical Institute, Kolkata

Abstract: In (k, n) visual cryptographic schemes (VCS), a secret image is encrypted into n pages of cipher text, each printed on a transparency sheet, which are distributed among n participants. The image can be visually decoded if any $k\,(\geq 2)$ of these sheets are stacked on top of one another, while this is not possible by stacking any $k-1$ or fewer sheets. We employ a Kronecker algebra to obtain necessary and sufficient conditions for the existence of a (k, n) VCS with a prior specification of relative contrasts that quantify the clarity of the recovered image. These are employed to settle certain conjectures on contrast optimal VCS for the cases k = 4 and 5. Furthermore, for k = 2, 3, we show how block designs, such as BIBD, PBIBD, etc., can be used to construct VCS which achieve optimality with respect to the average and minimum relative contrasts but require much smaller pixel expansions than the existing ones.

This is a joint work with Rahul Mukerjee, Indian Institute of Management, Calcutta.