CORR 99-57

Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels

Philip A. Eisen & Douglas R. Stinson

Abstract In 1994, Naoir and Shamir introduced an unconditionally secure method for encoding black and white images. this method, known as a threshold visual cryptography scheme (VCS), has the benefit of requiring no cryptographic computation on the part of the decoders. In a (k, n)-VCS, a share, in the form of a transparency, is given to n users. Any k users can recover the secret simply by stacking transparencies, but $k-1$ users can gain no information about the secret whatsoever.

In this paper, we first explore the issue of contrast, by demonstrating that the current definitions are inadequate, and by providing an alternative definition. This new definition motivates an examination of minimizing pixel expansion subject to fixing the VCS parameters h and l. New bounds on pixel expansion are introduced, and connections between these bounds are examined. The best bound presented is tighter than any previous bound. An analysis of connections between $(2, n)$ schemes and designs such as BIBD's, PDB's, and (r, λ)-designs is performed. Also, an integer linear program is provided whose solution exactly determines the minimum pixel expansion of a $(2, n)$-VCS with specified h and l.