Visual Cryptography (VC), proposed by Naor and Shamir in 1994, is a variation of the conventional secret sharing scheme. In VC, instead of a numerical secret key, a secret image is shared among participants in the form of images called shares. Each participant possesses his own share which cannot reveal the secret image being alone, making it necessary to stack more than one share of a qualified participant in order to reveal the secret image. Thus in VC the stacking of shares is equivalent to the decryption process, where neither extra computations nor previous knowledge are required to reveal the secret image. Until now some important VC schemes, such as the \((k,n)\)-VC scheme, the general access structure for VC and the extended VC (EVC), have been proposed. Unfortunately all schemes can be cheated, if one or more participants try to generate their fake shares to force the revealed secret image to be a faked one. In this paper, we propose a cheating prevention VC scheme, in which the shares can be identified and authenticated using the EVC scheme and watermarking techniques. In the proposed VC scheme, the share of each participant can be identified by its meaningful appearance instead of noise-like image used in the conventional VC scheme. For the purpose of authentication of each share two binary watermark images are encrypted using shift operation. Before the secret image is revealed, the validation of the shares must be carried out, extracting two watermark images. If they can be extracted correctly, the revealed secret image is considered as authentic; otherwise it is determined as a faked one. The simulation results show the desirable performance of the proposed EVC scheme.

**Keywords**

Visual cryptography, extended visual cryptography, cheating prevention, watermarking.