VISUAL SECRET SHARING SCHEMES

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

Naor and Shamir [NS94] developed what they called **visual secret sharing schemes**, which are an interesting visual variant of the ordinary secret sharing schemes.

Roughly speaking, the problem can be formulated as follows: There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible, but if fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately. The schemes are perfectly secure and easily implemented without any cryptographic computation. A further improvement allows each transparency (share) to be an innocent picture (e.g. a picture of a landscape or a picture of a building), thus concealing the fact that secret sharing is taking place.

In order to reduce the computation and furthermore secure the data, Naor and Shamir[1] proposed a new cryptology called visual cryptography in 1994. Without huge calculation, it can restore encrypted messages by stacking two shares via human visual system to identify. The first visual cryptography scheme is used for the black-and-white image in disorder to embed the confidential message. These disordered images are called “shares” that one of them may regard as the cipher text and the other treats as the key. Hackers cannot decrypt the secret message from one share.

COLOUR VISUAL CRYPTOGRAPHY

Visual cryptography scheme (VCS) is a kind of secret-sharing scheme which allows the encryption of a secret image into *n* shares that are distributed to *n* participants. The beauty of such a scheme is that, the decryption of the secret image requires neither the knowledge of cryptography nor complex computation.

Colour visual cryptography becomes an interesting research topic after the formal introduction of visual cryptography by Naor and Shamir in 1995. The authors propose a colour (*k*, *n*)-VCS under the visual cryptography model of Naor and Shamir with no pixel expansion, and a colour (*k*, *n*)-extended visual cryptography scheme ((*k*, *n*)-EVCS) under the visual cryptography model of Naor and Shamir with pixel expansion the same as that of its corresponding black and white (*k*, *n*)-EVCS.

Furthermore, the authors propose a black and white (*k*, *n*)-VCS and a black and white (*k*, *n*)-EVCS under the visual cryptography model of Tuyls. Based on the black and white schemes, the authors propose a colour (*k*, *n*)-VCS and a colour (*k*, *n*)-EVCS under the same visual cryptography model, of which the pixel expansions are the same as that of their corresponding black and white (*k*, *n*)-VCS and (*k*, *n*)-EVCS, respectively. The authors also give the experimental results of the proposed schemes, and compare the proposed scheme with known schemes in the literature.