


# Chapter 18

## Image Security Using Visual Cryptography


**Bala Krishnan R.**

 <https://orcid.org/0000-0002-4752-6400>  
SASTRA University (Deemed), India

**Manikandan G.**

SASTRA University (Deemed), India

**Rajesh Kumar N.**

 <https://orcid.org/0000-0001-5394-218X>  
SASTRA University (Deemed), India

**N. Rajesh**

Bule Hora University, Ethiopia

### ABSTRACT

*The use of digital image in a variety of disciplines has skyrocketed, particularly in multimedia, medicine, and social media. The integrity and confidentiality of digital images communicated over the internet can be jeopardized by a variety of security threats. As a result, the content of these digital images must be preserved at all costs for a variety of domain-specific applications. Visual cryptography scheme (VCs) is an image-based approach to encrypt the secret image in such a way, and human visual system (HVS) can be used to decrypt the image. The core concepts of visual cryptography and applications of several visual cryptography schemes are covered in this chapter. The authors describe a unique reversible data hiding method for protecting secret shares using a covering subset and recovering the secret image using an overlaying technique. This chapter also covers a comparative analysis of 2-out-of-n and 3-out-of-n visual cryptography schemes.*

DOI: 10.4018/978-1-7998-8892-5.ch018

## INTRODUCTION

A secret is piece of information or collection of data which is kept from the knowledge of any but the initiated or privileged. Secret contents are used in various fields such as, education, entertainment, manufacturing, logistics, healthcare and medicine. So the protection of secret content is very crucial in the modern internet communication. Secret sharing is an extra special method as compared to conventional scheme. Secret sharing is a process which a secret can be distributed between groups of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a share. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated. Within a secret sharing scheme, the secret is divided into a number of shares and distributed among  $n$  persons. When any  $k$  or more of these persons (where  $k \leq n$ ) bring their shares together, the secret can be recovered. However, if  $k - 1$  persons attempt to reconstruct the secret, they will fail. Secret sharing involves four major steps, which is shown in Table 1.

Table 1. Major steps in secret sharing

Steps	Description
Secret shares	Non-overlapped piece of information from the secret image
Image Splitter	The process is responsible for the division of secret image
Coalition	A sub collection of shares that need to satisfy the required condition
Stacker	A process responsible for reconstructing the secret image

## Principle of Secret Splitting

Secret sharing is introduced by Israeli cryptographer Adi Shamir and American Cryptographer George Blakely in 1979. The main theme of this algorithm is to split the secret into multiple parts and distribute the secret shares among group of participants. Each part contains a small amount of original information in the form of invisible mode and they don't reveal any information. The secret is reconstructed by sufficient number of qualified shares. A simple secret sharing divides a message between two participants. Consider the following scenario:

A sender named as 'Danie' has a secret message  $M$ , represented as an integer that he would like to share the secret between two receivers Alice and Bob. There will be other way to reconstruct the secret without the participation of both receivers. The following is the solution of the above statement.

Let ' $r$ ' be a random number. Then  $r$  and ' $M - r$ ' are independently random. Daniel gives ' $M - r$ ' to the first recipient and  $r$  to the second recipient as their shares. Each share reveals no information about the number, he message  $M$ . To recover the message, Alice and Bob have to simply add their shares together.

An alternative method is used by Daniel to split a message between Alice and Bob:

1. Daniel creates a random-bit string  $R$ , of the same length as the message  $M$ .
2. He XORs the message ( $M$ ) with random-bit string ( $R$ ) to create  $S$ . i.e.,  $M \oplus R = S$ .

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/image-security-using-visual-cryptography/314003](http://www.igi-global.com/chapter/image-security-using-visual-cryptography/314003)

## Related Content

---

### Line Parameter based Word-Level Indic Script Identification System

Pawan Kumar Singh, Supratim Das, Ram Sarkar and Mita Nasipuri (2016). *International Journal of Computer Vision and Image Processing* (pp. 18-41).

[www.irma-international.org/article/line-parameter-based-word-level-indic-script-identification-system/171129](http://www.irma-international.org/article/line-parameter-based-word-level-indic-script-identification-system/171129)

### A Semi-Supervised Metric Learning for Content-Based Image Retrieval

I. Daoudi and K. Idrissi (2011). *International Journal of Computer Vision and Image Processing* (pp. 53-63).

[www.irma-international.org/article/semi-supervised-metric-learning-content/59878](http://www.irma-international.org/article/semi-supervised-metric-learning-content/59878)

### Machine Learning for Automated Polyp Detection in Computed Tomography Colonography

Abhilash Alexander Miranda, Olivier Caelen and Gianluca Bontempi (2010). *Biomedical Image Analysis and Machine Learning Technologies: Applications and Techniques* (pp. 54-77).

[www.irma-international.org/chapter/machine-learning-automated-polyp-detection/39555](http://www.irma-international.org/chapter/machine-learning-automated-polyp-detection/39555)

### Adapted Approach for Omnidirectional Egomotion Estimation\*

A. Radgui, C. Demonceaux, E. Mouaddib, M. Rziza and D. Aboutajdine (2011). *International Journal of Computer Vision and Image Processing* (pp. 1-13).

[www.irma-international.org/article/adapted-approach-omnidirectional-egomotion-estimation/53713](http://www.irma-international.org/article/adapted-approach-omnidirectional-egomotion-estimation/53713)

### A Hybrid Lossless-Lossy Binary Image Compression Scheme

Saif alZahir and Syed M. Naqvi (2013). *International Journal of Computer Vision and Image Processing* (pp. 37-50).

[www.irma-international.org/article/a-hybrid-lossless-lossy-binary-image-compression-scheme/103957](http://www.irma-international.org/article/a-hybrid-lossless-lossy-binary-image-compression-scheme/103957)