About a visual secret sharing scheme

Ruxandra-Florentina Olimid

Faculty of Mathematics and Computer Science
University of Bycharest
Romania

ruxandra.olimid@fmi.unibuc.ro

November 18, 2010

Outline

Visual Secret Sharing Schemes

SSS(Secret Sharing Scheme) - a secret is split between n participants so that only the authorised groups of participants are able to reconstruct the secret, by combining their shares;

Visual Secret Sharing Schemes

SSS(Secret Sharing Scheme) - a secret is split between n participants so that only the authorised groups of participants are able to reconstruct the secret, by combining their shares;
Phases:

- Shares computation;
- Shares distribution to participants;
- Secret reconstruction.

Visual Secret Sharing Schemes

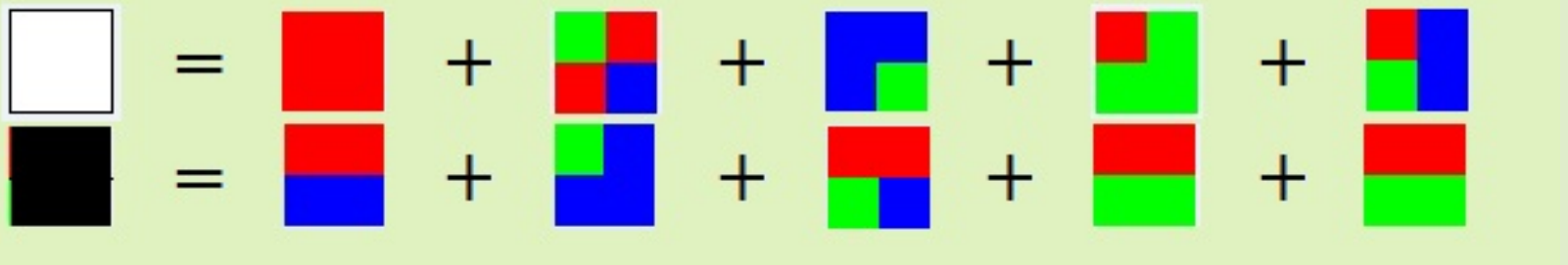
SSS(Secret Sharing Scheme) - a secret is split between n participants so that only the authorised groups of participants are able to reconstruct the secret, by combining their shares;
Phases:

- Shares computation;
- Shares distribution to participants;
- Secret reconstruction.

VSS(Visual Secret Sharing Scheme) - a SSS for which the secret, and therefore the components, are images;

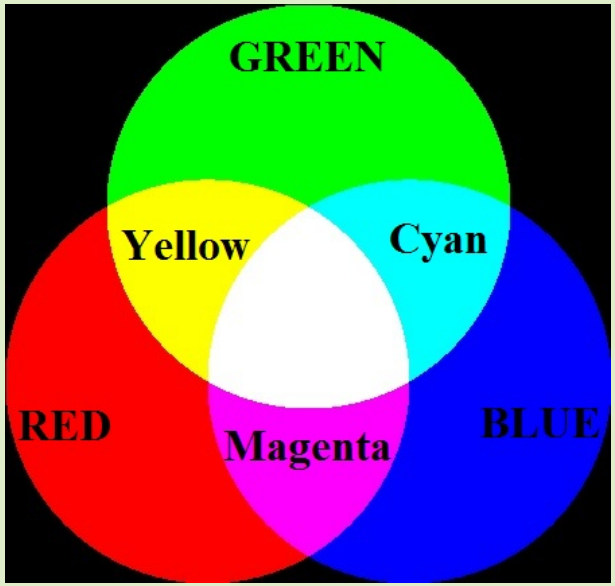
Scheme Presentation

- The secret: a Black and White image;
- The shares: n ($n \geq 3$) RGB-colored images of the same size.



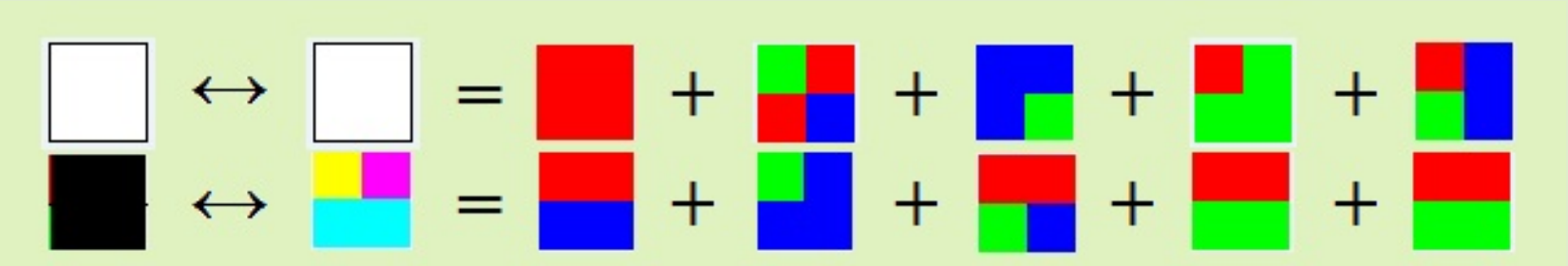
RGB Model

- By mixing 2 colors, Y, M or C are obtained;
- R, G and B are all needed in order to obtain White;



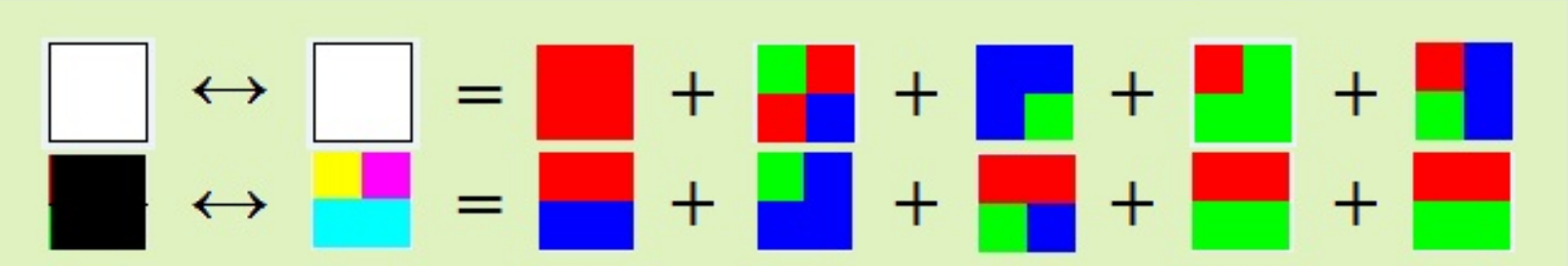
Scheme Presentation

- A White pixel of the reconstructed image correspond to a White pixel of the secret image;
- All the other pixels are considered Black.



Scheme Presentation

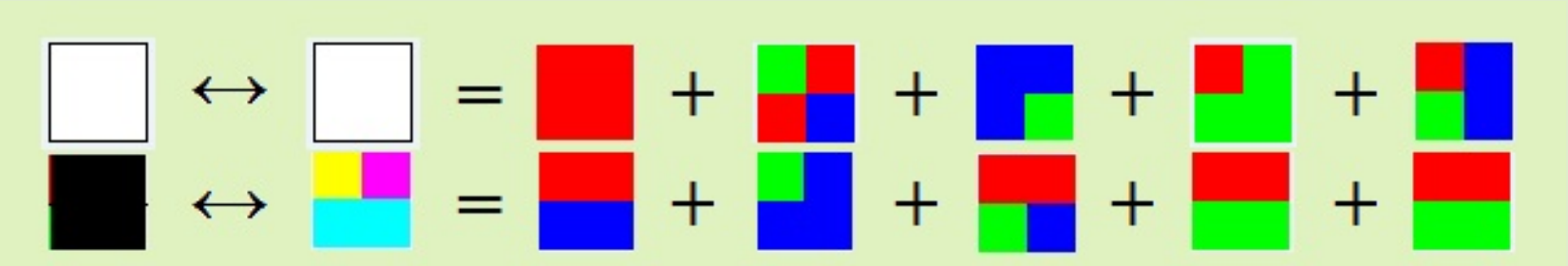
- A White pixel of the reconstructed image correspond to a White pixel of the secret image;
- All the other pixels are considered Black.



1. How are the shares computed?

Scheme Presentation

- A White pixel of the reconstructed image correspond to a White pixel of the secret image;
- All the other pixels are considered Black.



1. How are the shares computed?
2. How is the secret reconstructed from shares?

Scheme Analysis

Scheme's parameters and efficiency:

- The secret must be split into at least 3 shares ($n \geq 3$);
- The size of one share equals the size of the secret;
- The reconstructed image maintain the same size and ratio of the secret image.

Scheme Analysis

Scheme's parameters and efficiency:

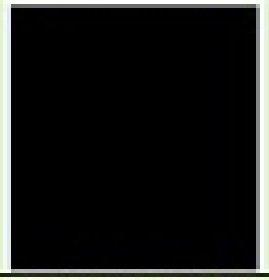
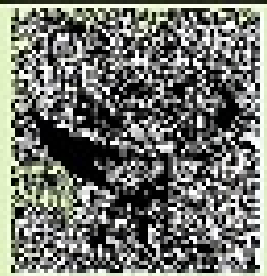
- The secret must be split into at least 3 shares ($n \geq 3$);
- The size of one share equals the size of the secret;
- The reconstructed image maintain the same size and ratio of the secret image.

Scheme's Secrecy:

- $k = 1$ or $k = 2$: perfect secrecy;
- $3 \leq k < n$: partial information is revealed;
- $k = n$: the secret image is perfectly recovered.

Implementation and results

- Implemented in Python: PIL (Python Image Library), IDLE (Python Integrated Development Environment);
- Pretty fast processing;
- Experimental results supports the theory.

No of used shares(k)	Color computed secret	Black and white computed secret
2		
3		
4		

Conclusions

The presented secret sharing scheme:

- is used for sharing Black and White secret images using R,G,B-colored components;
- maintains the actual size and ratio of the secret;
- is storage-efficient;
- provides perfect secrecy for 1 or 2 participants;
- provides perfect recovery of the secret when all participants cooperate;
- can be successfully used in practice.

References

[1] Y.C.Hou, *Visual Cryptography for Color Images:*
http://ma1.eiius.es/miembros/valvarez/proyectos/viscryptcolor.pdf
[2] R.Ito, H.Kuwakado, H.Tanaka, *Image Size Invariant Visual Cryptography:*
citeseer.ist.psu.edu/353362.html
[3] M.Naor, A.Shamir, *Visual Cryptography:*
http://www.cs.ncuu.edu.tw/ raylin/UndergraduateCourse/Contemporary Cryptography/Spring2009/VisualCrypto.pdf
[4]Python Imaging Library(PIL):
www.pythonware.com/products/pil

Thank you!

Questions