**ACS 54500 Crypto and Network Security**

**MIDWAY – REPORT**

* Select two good papers.

1. Why are the papers good?

Papers that I was looking were in the realm of visual cryptography. Visual cryptography is a cryptographic approach that encrypts visual information (images, text, etc.) so that the decrypted information appears as a visual image. Below mentioned documents were not only informative but challenging as there was a topic to be studied and something that was known but not insighted. These papers were well cited and were published at well known conferences in 2006 and 2007 respectively.

1. What are the links to papers?

* **Halftone visual cryptography**
* **Cited by 525.**
* Zhi Zhou, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography," in**IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, Aug. 2006, doi: 10.1109/TIP.2006.875249**.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1658106&isnumber=34713>

Abstract: Visual cryptography encodes a secret binary image (SI) into n shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the n shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography was proposed recently to construct meaningful binary images as shares using hypergraph colourings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date.

* **Sharing multiple secrets in visual cryptography.**
* **Cited by 273.**
* Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, Kun Chen, Sharing multiple secrets in visual cryptography, Pattern Recognition, Volume 40, Issue 12, 2007, Pages 3633-3651, ISSN 0031-3203.

<https://doi.org/10.1016/j.patcog.2007.03.012> (<https://www.sciencedirect.com/science/article/pii/S0031320307001380>)

Abstract: The secret sharing schemes in conventional visual cryptography are characterized by encoding one shared secret into a set of random transparencies which reveal the secret to the human visual system when they are superimposed. In this paper, we propose a visual secret sharing scheme that encodes a set of x⩾ 2 secrets into two circle shares such that none of any single share leaks the secrets and the x secrets can be obtained one by one by stacking the first share and the rotated second shares with x different rotation angles. This is the first true result that discusses the sharing ability in visual cryptography up to any general number of multiple secrets in two circle shares.

Keywords: Secret sharing; Visual cryptography; Visual multi-secret sharing.

1. What are the links to code repository?

* <https://github.com/anushka23g/Half-Tone-Visual-Cryptography>

Visual cryptographic schemes (VCS) allow one(at the sender side) to encrypt a secret picture (image) into different share images. Here no share image does uncover any knowledge concerning the original secret image. This work proposes a visual cryptography encryption framework. A color image to be protected is taken as input and then this image is decomposed into three separate monochromatic images based on CMY color space. The computer simulation demonstrates that the visual nature and tone (in terms of quality) of the acquired halftoned shares is acceptable.

* <https://github.com/Qbicz/multi-secret-sharing>

Multi-secret-sharing is a tool for splitting multiple secrets among multiple stakeholders. It uses cryptography to divide secret data into multiple parts in such a way that compromising even a few secret parts does not endanger security of a secret. The parts, or secret shares are saved as JSON files and can be later distributed to several people or backed up on separate disks and online storage facilities.

* Report the progress.

1. Have you finished the first two passes of reading the paper? Any questions?

Yes, I have finished the first two passes of reading the paper. No questions as of late, still going through visual cryptography’s applications through halftone visual cryptography as it’s an emerging encryption technique for information hiding using images, etc.

1. What are the main ideas and contributions of the paper?

Few of the main ideas were of course the simulation showing the visual quality of the obtained halftone shares which were observed and attained by the available visual cryptography method known till date by encoding a secret binary image into n shares of random binary patterns. The hidden image can be visually decrypted by superimposing a qualified subset of transparencies, but the superposition of a banned subset yields no secret information.

1. What are the possible challenges for you to re-implement the experiments in the paper?

Despite the fact that it was designed just for binary images, several papers and research articles have been published on its use in grayscale and colorful images. In this paper, we look at one such method in which a picture is color decomposed into Cyan, Magenta, and yellow hues, and then the individual decomposition is done using visual cryptography. As of now, I didn’t find anything challenging with the dog-pic that was part of this project’s output. Soon I would try to implement it with a variety of more pictures and ensure that individual cover pictures do not reveal any information about a secret image to hackers.

1. How much re-implementation of the work have you done?

I followed the steps that were used for implementing the project in the first place on visual studio code as it’s a python-based project

A picture containing grass, outdoor, dog, mammal

Description automatically generated

The secret image that was encoded into.

A picture containing text

Description automatically generated

Haftoned Images.

A picture containing text, monitor, television, screen

Description automatically generated

Shared Images 1, 2 & 3.

A picture containing text, green, display

Description automatically generated

Decoded by superimposing these three shares.

Decoded image.

The research looks at one such method, in which an image is color decomposed into Cyan, Magenta, and Yellow hues, and then the individual breakdown is done using visual cryptography.