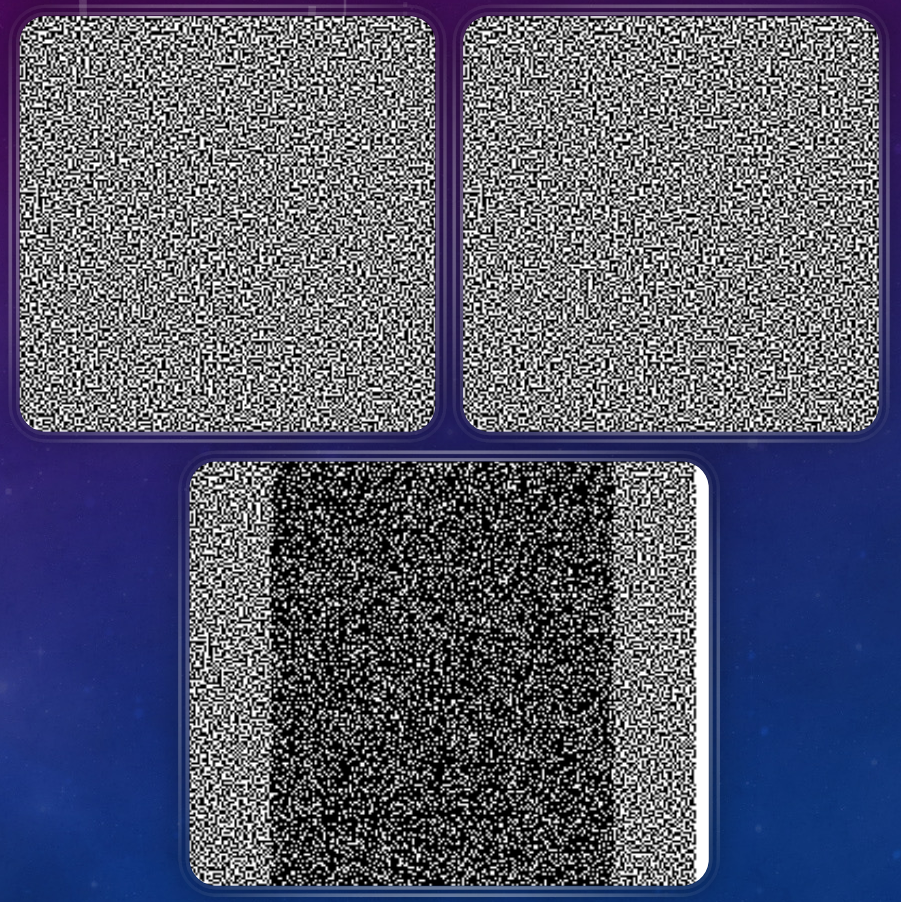
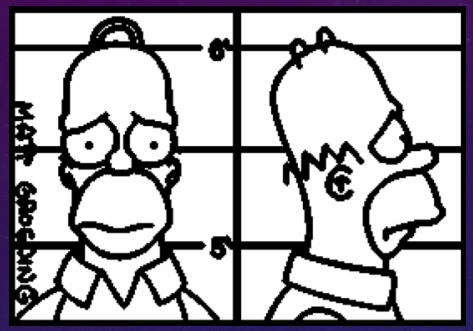
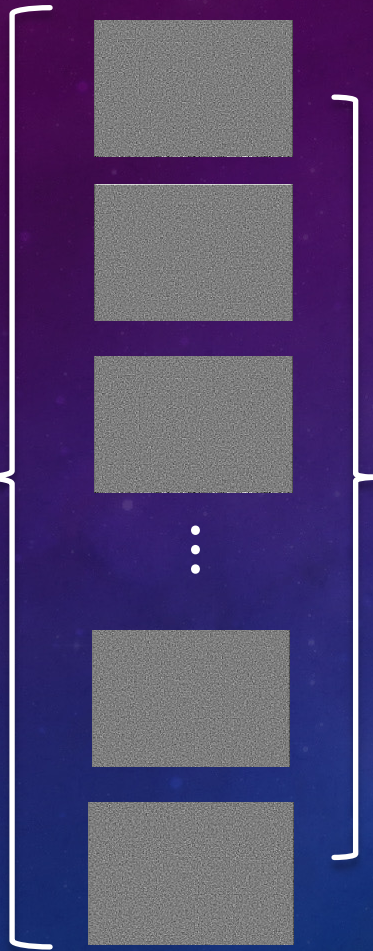
VISUAL CRYPTOGRAPHY

SPARSH GUPTA, MARK BELANGER, SIDNEY TAYLOR

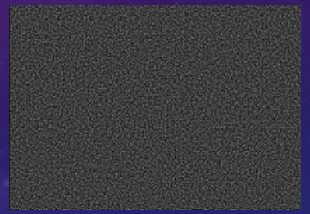




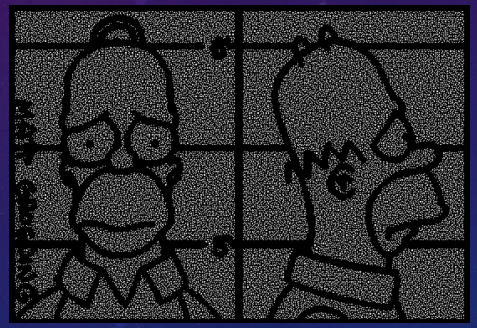
Original image



n encrypted shares



Less than k shares overlayed



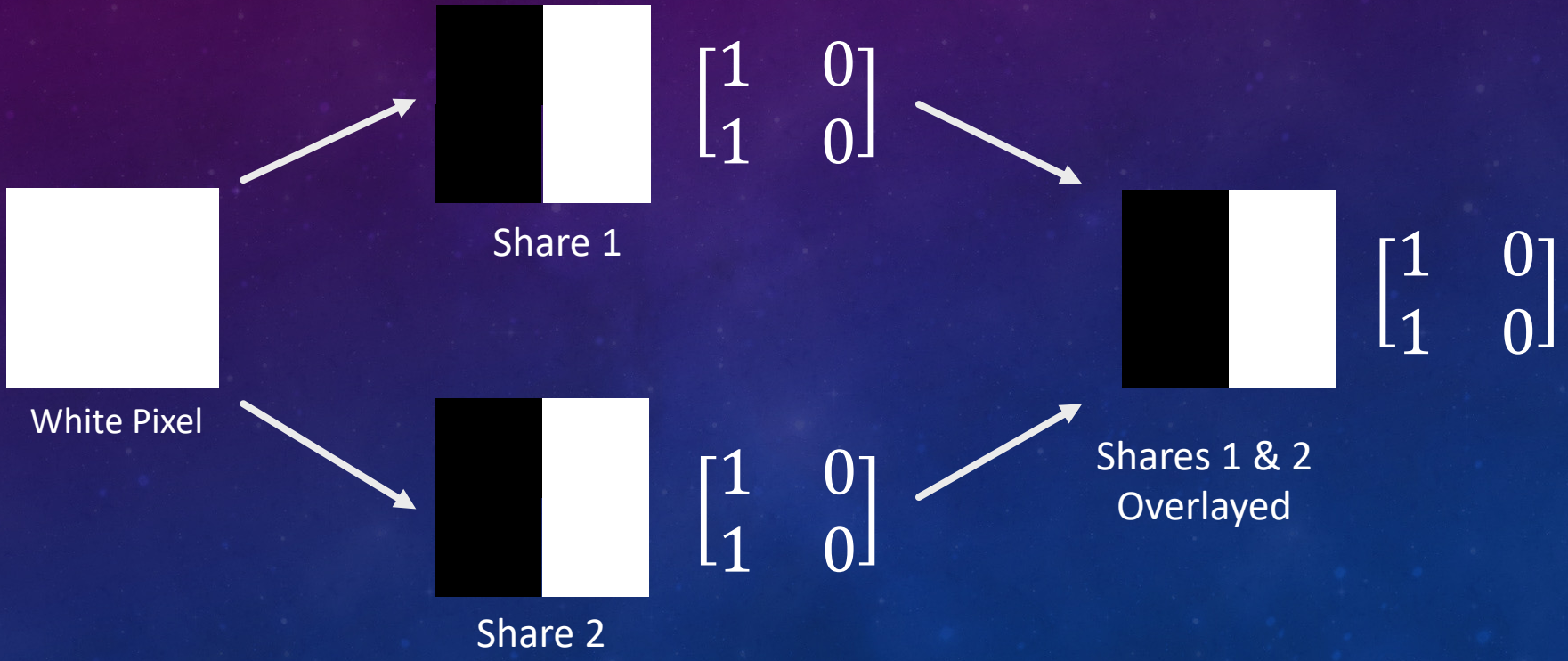
k shares overlayed (decrypted image)

[5]

SHAMIR'S VISUAL CRYPTOGRAPHY SCHEME

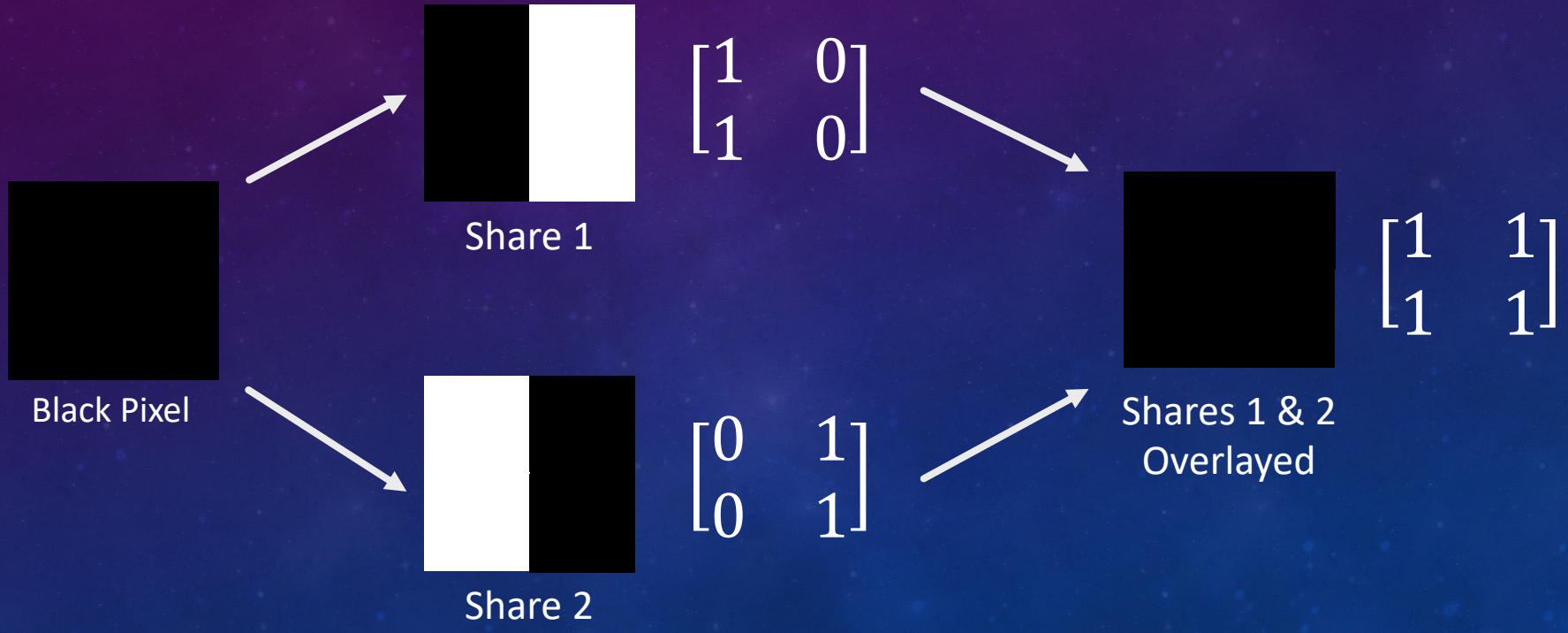
HOW WHITE PIXELS ARE HANDLED

Shares are made of the same subpixel arrangement



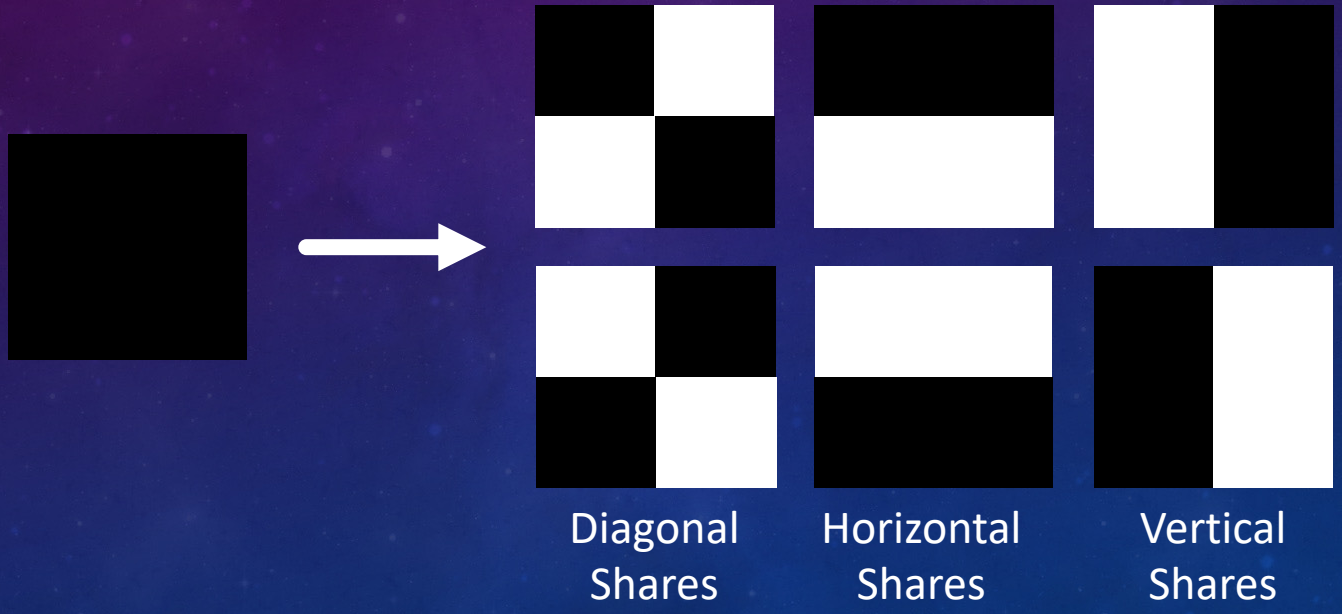
HOW BLACK PIXELS ARE HANDLED

Shares are made of reciprocal subpixel arrangements

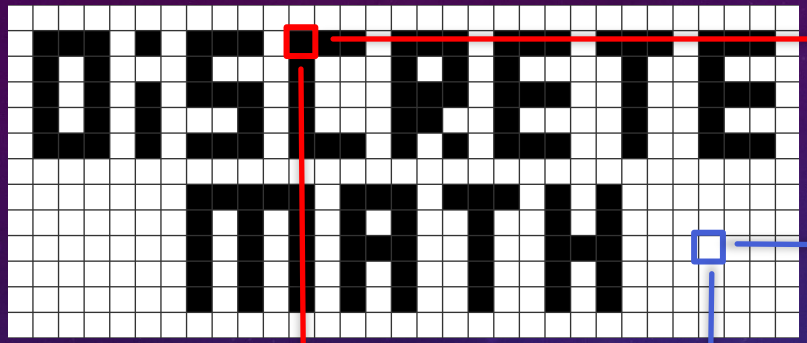


PIXEL EXPANSION (BLACK PIXEL SHARES)

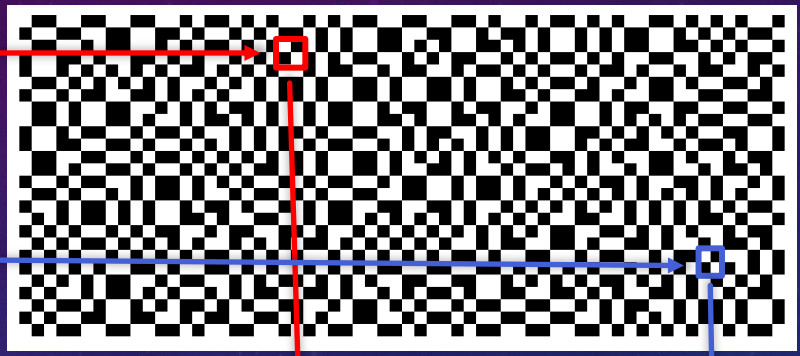
- Each pixel is broken into sub-pixels, and that get encoded



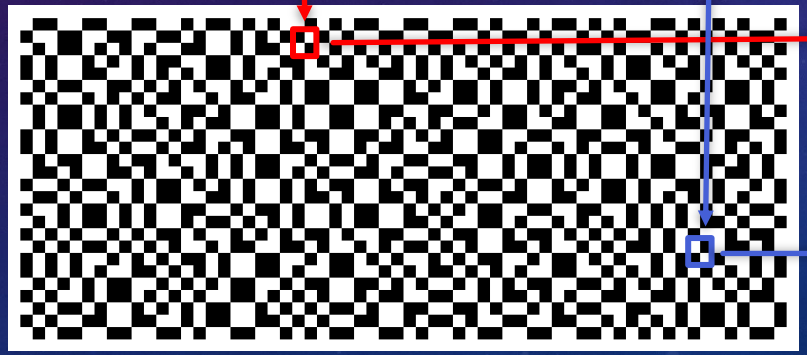
SHAMIR'S SCHEME EXAMPLE (PIXEL EXPANSION)

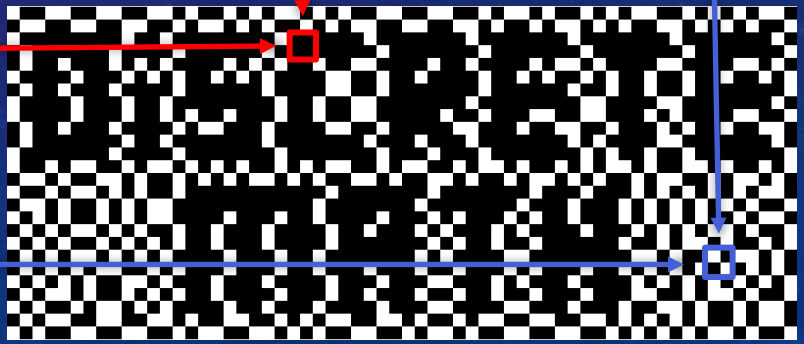


Share 2

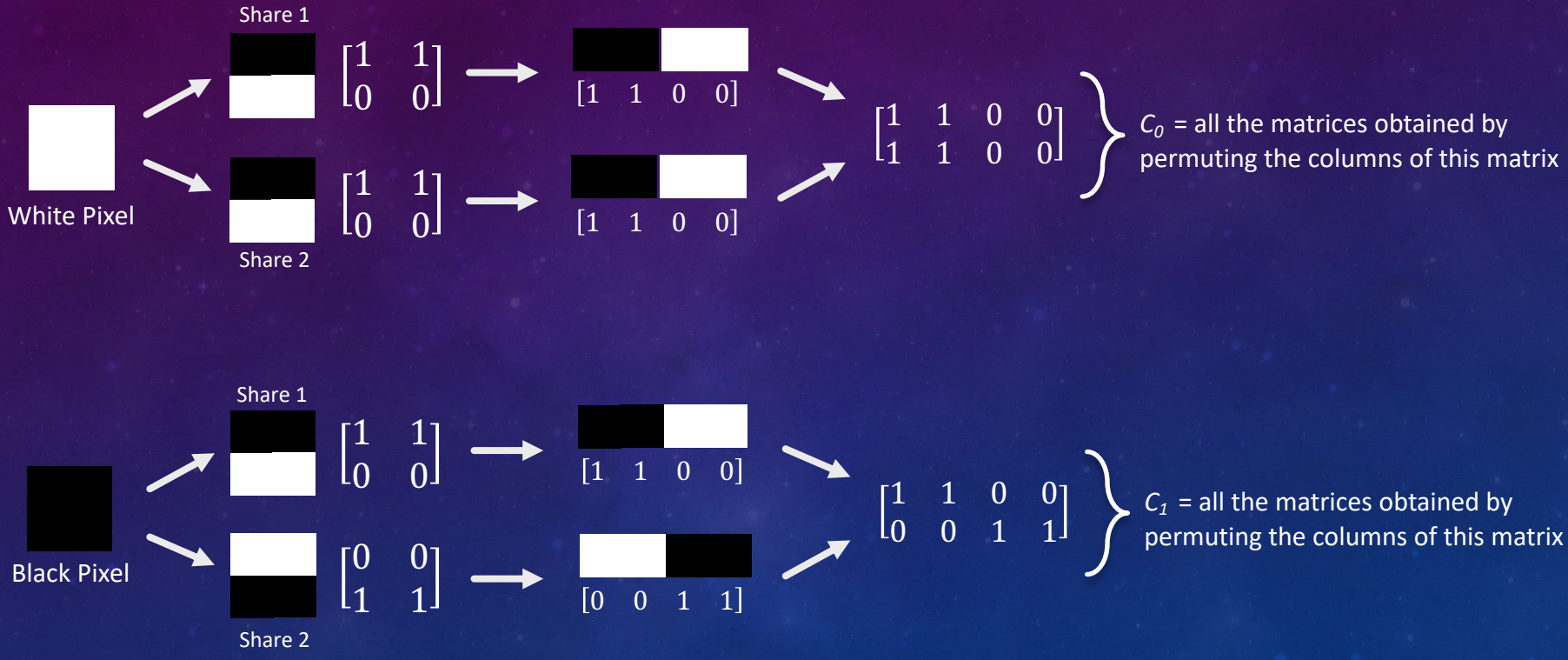


Share 1

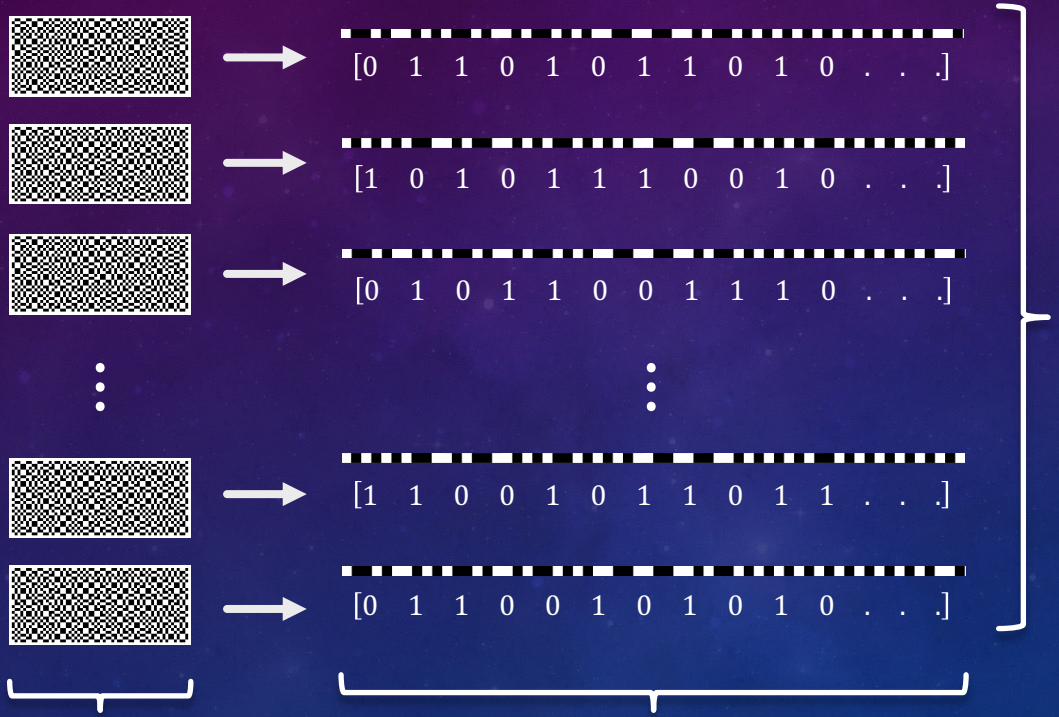




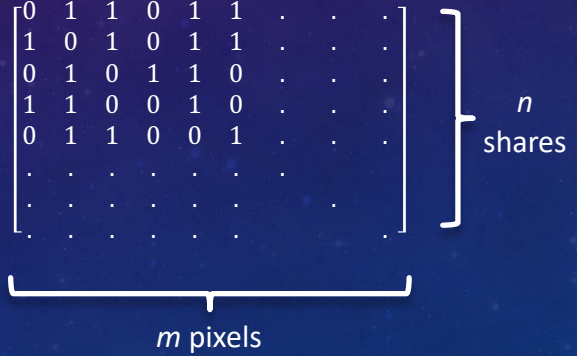
GENERAL PIXEL ENCODING MATRIX (FOR 2 SHARES)



K OUT OF N SCHEME – DECODING SHARES



$S_0 / S_1 = s_{i,j}$ (m x n)



S_0 => white pixel shares
S_1 => black pixel shares

K OUT OF N SCHEME - DECRYPTING IMAGE

$S_0 =$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & . & . & . \\ 1 & 0 & 1 & 0 & 1 & 1 & . & . & . \\ 0 & 1 & 0 & 1 & 1 & 0 & . & . & . \\ 1 & 1 & 0 & 0 & 1 & 0 & . & . & . \\ 0 & 1 & 1 & 0 & 0 & 1 & . & . & . \\ . & . & . & . & . & . & . & & \\ . & . & . & . & . & . & & . & \\ . & . & . & . & . & . & & & . \end{bmatrix}$$

$S_1 =$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & . & . & . \\ 1 & 1 & 0 & 0 & 0 & 1 & . & . & . \\ 0 & 0 & 1 & 0 & 1 & 0 & . & . & . \\ 0 & 1 & 1 & 0 & 0 & 1 & . & . & . \\ 1 & 0 & 1 & 0 & 0 & 1 & . & . & . \\ . & . & . & . & . & . & . & & \\ . & . & . & . & . & . & & . & \\ . & . & . & . & . & . & & & . \end{bmatrix}$$

Column vector *V*

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & . & . & . \\ 1 & 1 & 1 & 0 & 1 & 1 & . & . & . \\ 0 & 1 & 1 & 1 & 1 & 0 & . & . & . \\ 1 & 1 & 1 & 0 & 1 & 1 & . & . & . \\ 1 & 1 & 1 & 0 & 0 & 1 & . & . & . \\ . & . & . & . & . & . & . & & \\ . & . & . & . & . & . & & . & \\ . & . & . & . & . & . & & & . \end{bmatrix}$$

Boolean OR result
(between each row of S_0 and S_1)

$$[10 \quad 21 \quad 5 \quad 23 \quad 35 \quad 8 \quad 27 \quad 19 \quad . \quad . \quad .]$$

If *H(V)* <= *d*

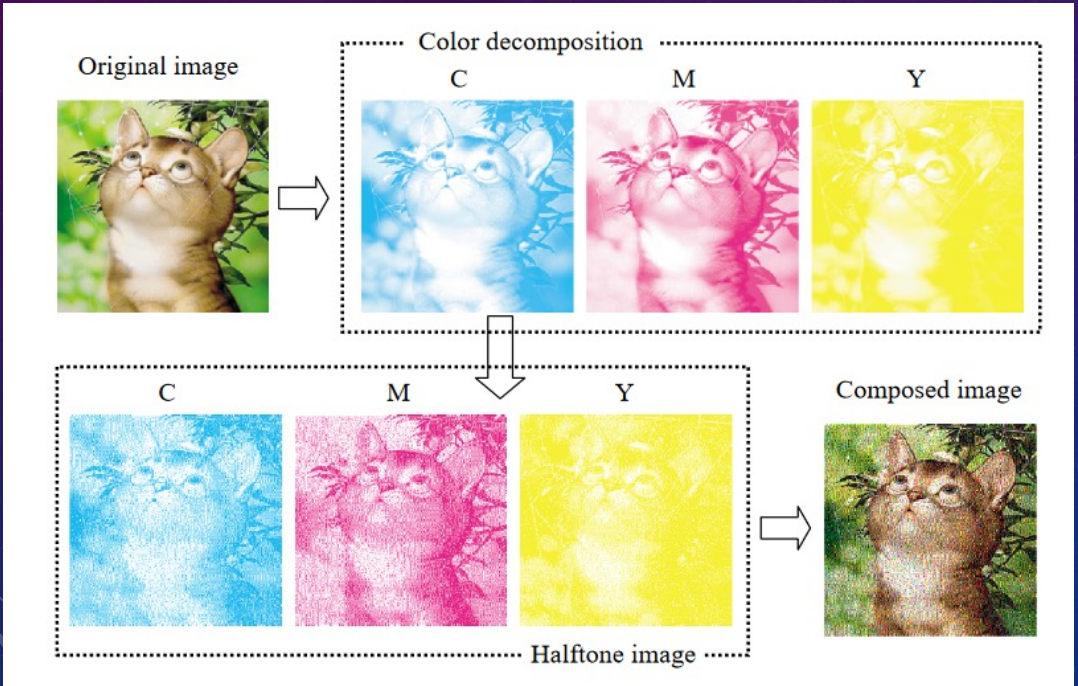
If *H(V)* < *d* - αm

(where *H(V)* is the hamming weight of *V*,
0 <= *d* <= *m* and $\alpha > 0$)

$$\alpha = \frac{1}{2^{k-1}}$$

WHAT IF WE EXPAND THIS ALGORITHM FOR COLOR IMAGES?

DECOMPOSING COLOR IMAGES

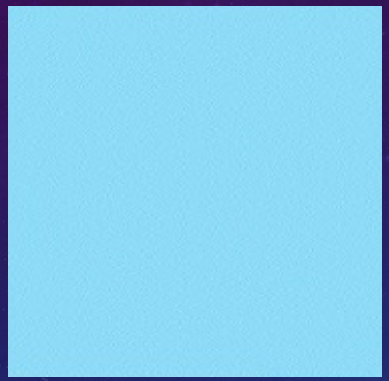


Color images can be represented using combinations of cyan, magenta, and yellow

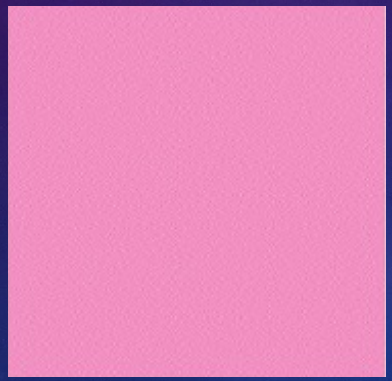
[4]

HOW IT WORKS

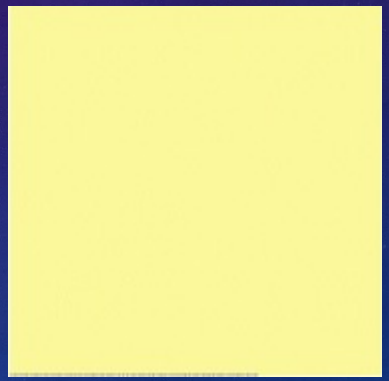
Decompose image into CMY (i.e each pixel looks something like (1, 0, 1))→ pixel-by-pixel encryption into the 4 shares with pixel expansion



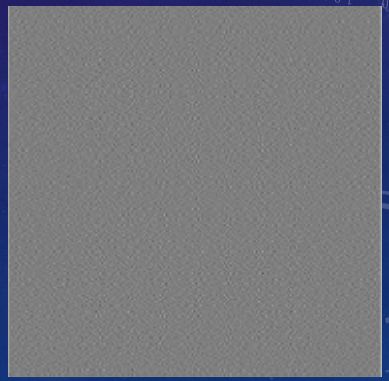
Cyan Share



Magenta Share



Yellow Share

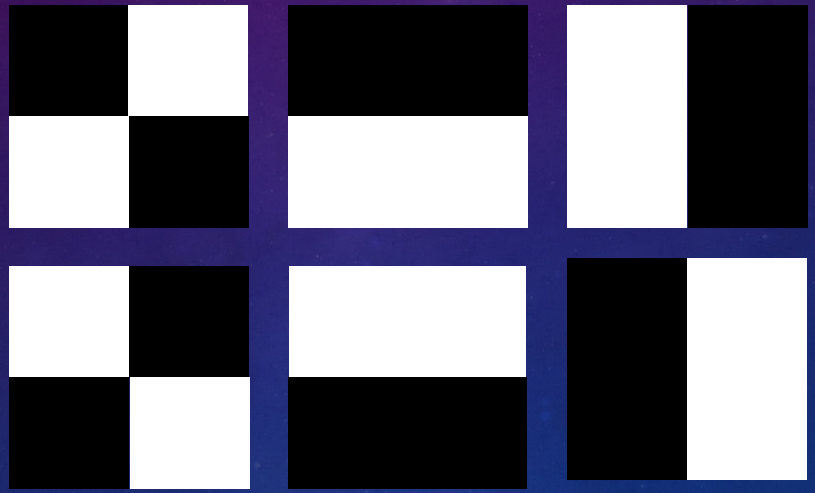


Black Share

[4]

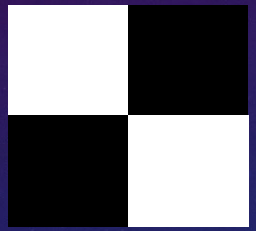
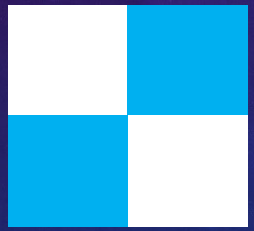
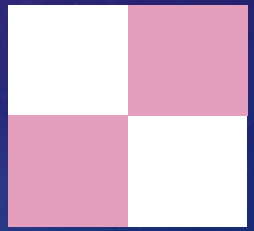
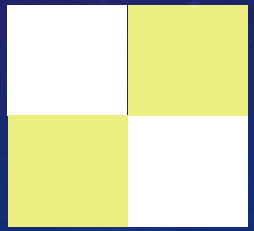
CREATING THE BLACK SHARE

Step 1: Select one of these for each pixel:



ARRANGEMENT OF COLOR SHARES

- Depends on the black share
- CMY fills white space depending on if it needs to be shown

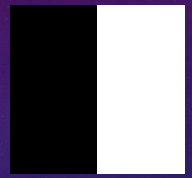
COLORS THAT CAN BE CREATED

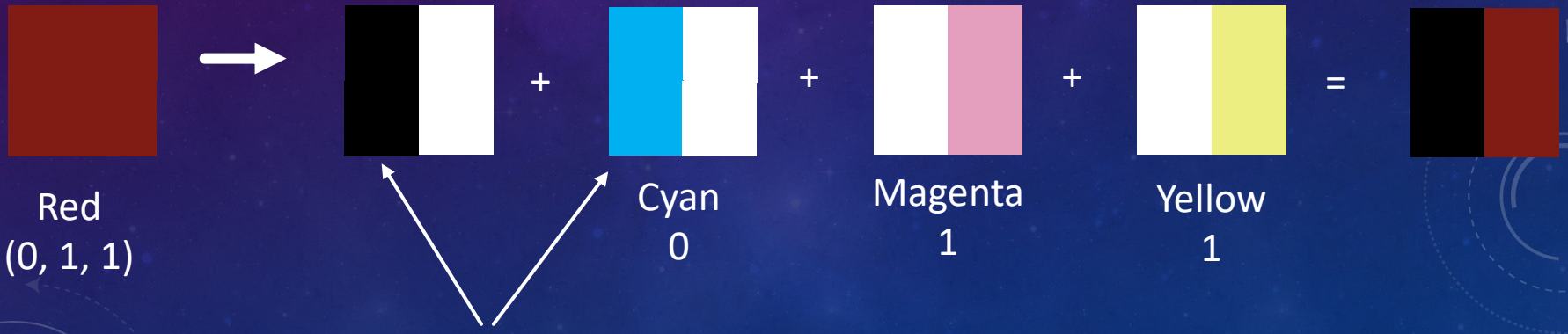
Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

[4]

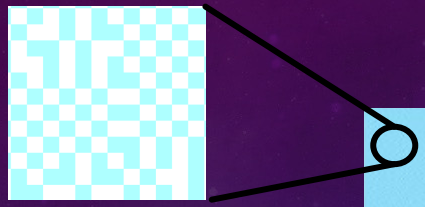
RED PIXEL EXAMPLE

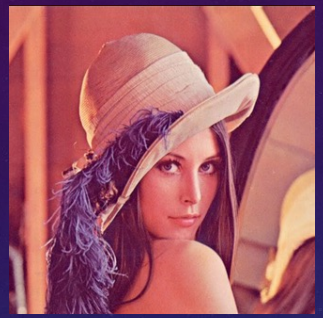
If black share subpixel group is





COLOR IMAGE VISUAL CRYPTOGRAPHY EXAMPLE





Original image

Cyan Share

Magenta Share

Yellow Share

Black Share

Decrypted image

[4]

THANK YOU!

QUESTIONS?

REFERENCES

[1] https://www.cs.jhu.edu/~fabian/courses/CS600.624/NaorShamir-VisualCryptography.pdf

[2] https://www.researchgate.net/publication/353374619_An_overview_of_visual_cryptography_techniques

[3] https://www.ciphermachinesandcryptology.com/en/visualcrypto.htm

[4] https://www.sciencedirect.com/science/article/pii/S0031320302002583#SEC3

[5] https://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf

[6] https://fardapaper.ir/mohavaha/uploads/2018/12/Fardapaper-A-Comprehensive-Study-of-Visual-Cryptography.pdf

[7] https://www.101computing.net/visual-cryptography/