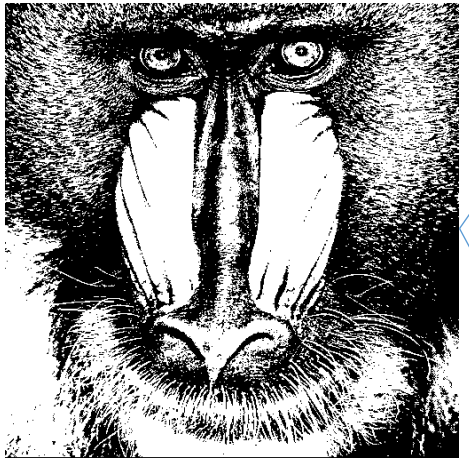
Byzantine Resilient Waves Interference-based Visual Encryption Scheme

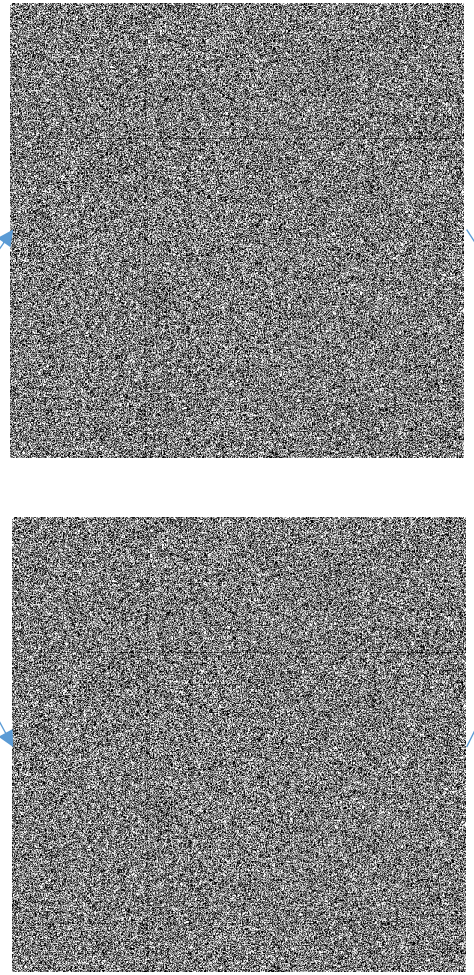
Alexander Fok,
Shlomi Dolev and Michael Segal

Ben-Gurion University of the Negev, Israel

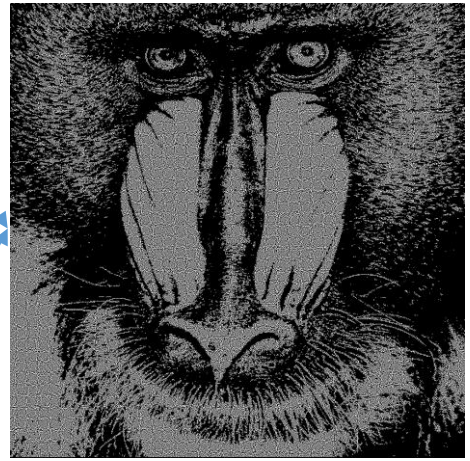
VES Background



Original Image



Original Image Shares – random Yellow and Blue pixels



Recovered Image – grey pixels

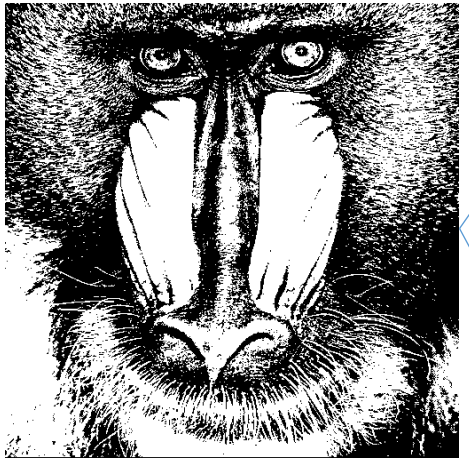
VES Pixel Encoding, Naor and Shamir Definition - Black = 1 White = 0

Share 1	Share 2	Stack 1 & 2 - OR
		
		

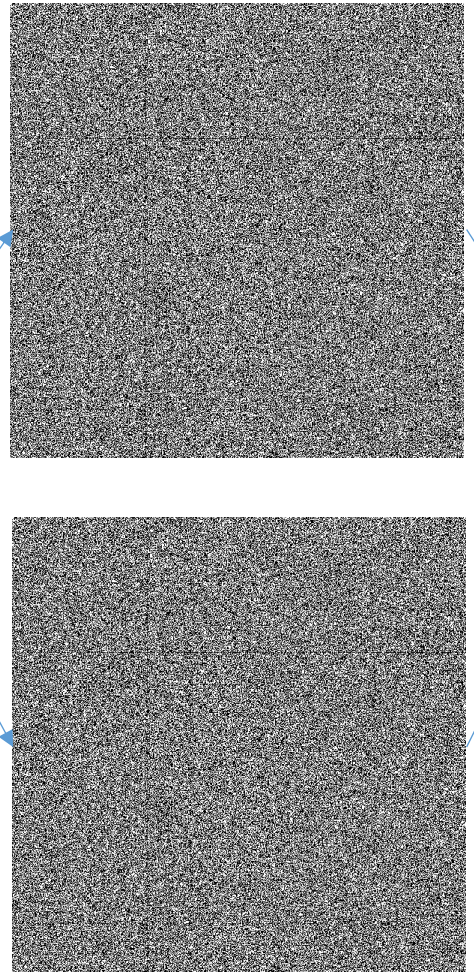
VES Properties

- Advantages
  - Perfect information-theoretic security against honest and curious adversaries
  - Computational efficiency
- Limitations
  - Perfect Color Use Limitation
  - Byzantine Adversary Vulnerability

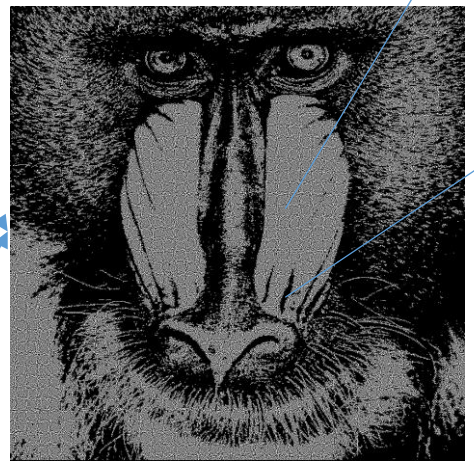
VES Perfect Color Use Limitation



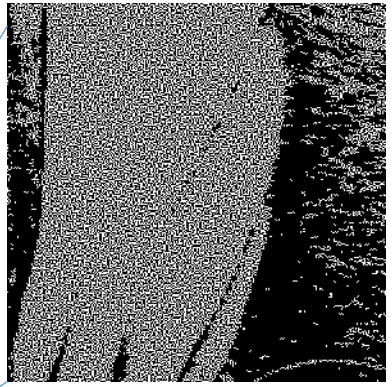
Original Image



Original Image Shares – random Yellow and Blue pixels

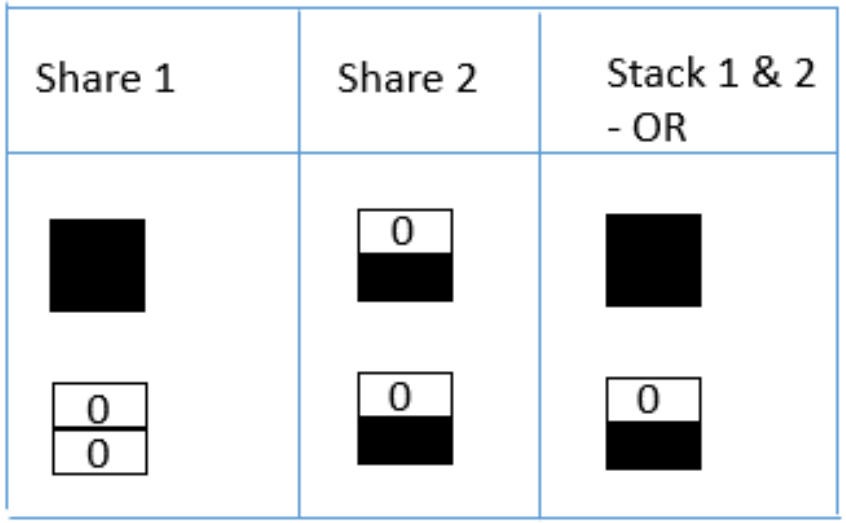


Recovered Image – grey pixels



VES Perfect Color Use Limitation

- visual effect of a black subpixel can not be undone
- monotonicity



Byzantine Adversary Vulnerability

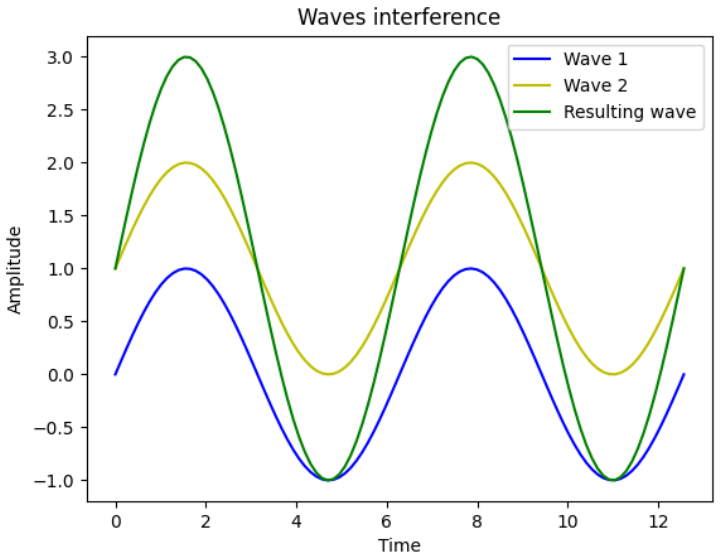
- Byzantine adversary changes single white sub pixel of the share 1 to a black => pixel becomes black
- Monotonicity – no way to detect or correct Byzantine adversary action

Our Solution

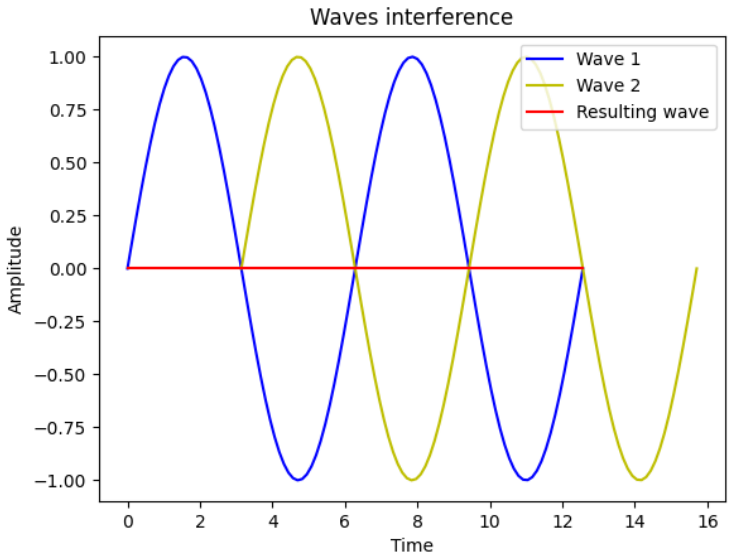
- Waves Interference-based Visual Encryption Scheme

Waves Interference Types

Constructive Interference



Destructive Interference



Definitions

- Represent VES shares as wave signals $S_i = (A_i, P_i)$
- Introduce phase and amplitude to control the waves interaction
- $A_i = 1$
- $P_i = \in \{P_1, P_2\}$
- A – represents reconstructed pixel amplitude
- S - represents reconstructed pixel wave signal

Reconstructed Pixel Amplitude A Calculation

- $A = \sum_1^n (A_i, P_i)$
- Examples
  - $S = \{P_1, P_2, P_1\} = 1{,}0 \Rightarrow \mathrm{A} = 1$
  - $S = \{P_2, P_2, P_1\} = 0{,}1 \Rightarrow \mathrm{A} = 1$

Two Shares Model

0 Black pixel

2 2 White pixel

Share 1	Share 2	Stack 1 & 2
1	1	2 0 =2
1	1	0 0 =0
1	1	0 0 =0
1	1	0 2 =2

N Shares Model – Even N

0 Black pixel

2 2 White pixel

k	C_k^n	Share Examples	Stack 1 & 2
0	1	1 1 1 1	0 4 =4
1	4	1 1 1 1	1 3 =3
2	6	1 1 1 1	2 2 =0
3	4	1 1 1 1	3 1 =3
4	1	1 1 1 1	4 0 =4

N Shares Model – Odd N

1 Black pixel

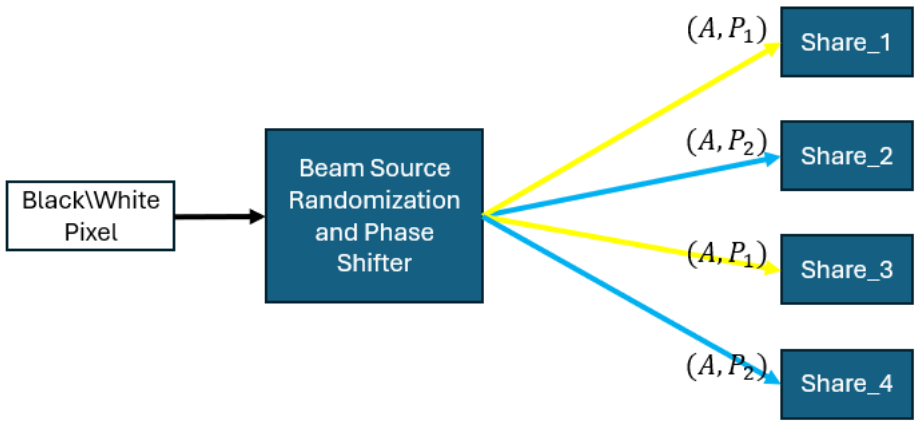
3 3 White pixel

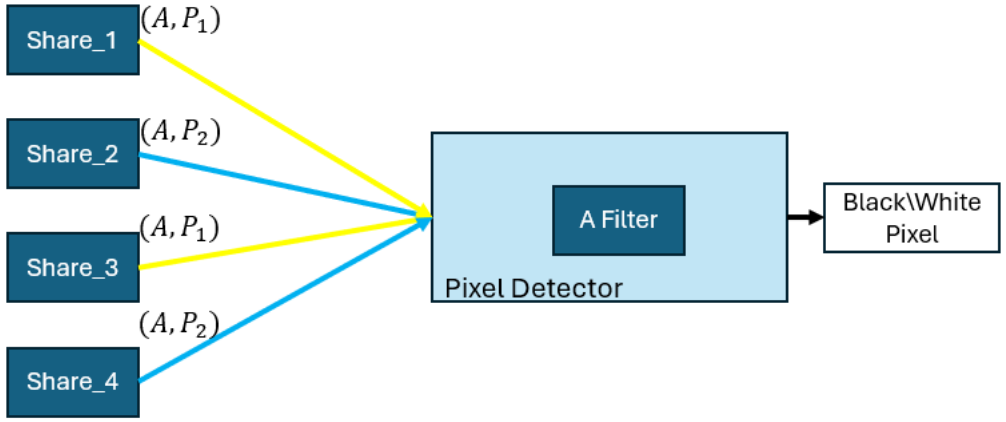
k	C_k^n	Share Examples	Stack 1 & 2
0	1	1 1 1 1 1	0 5 =5
1	5	1 1 1 1 1	1 4 =2
2	10	1 1 1 1 1	2 3 =1
3	10	1 1 1 1 1	3 2 =1
4	5	1 1 1 1 1	4 1 =3
5	1	1 1 1 1 1	5 0 =5

Implementation - Amplitude Threshold Filter

- $\hat{A} = \begin{cases} 0, if\ A < F \\ A, otherwise \end{cases}$

Implementation





Security Model

- Security goal 1 - adversary that controls less than ***d*** agents can not reveal any information about the secret image
- Security goal 2 – less than ***b*** byzantine adversaries can not affect the original image reconstruction

Byzantine Adversaries Resiliency

- Single Byzantine adversary alters the signal amplitude - A_i
- Single Byzantine adversary alters the signal phase - P_i

Byzantine Adversaries Resiliency

- Even N, N=6

k	Share Examples	Original Sum	Flipped Share Sum	Filtered Sum
0	1 1 1 1 1 1 | 1	=6	=4	=4
1	1 1 1 1 1 1 | 1	=4	=6	=6
2	1 1 1 1 1 1 | 1	=2	=4	=4
3	1 1 1 1 1 1 | 1	=0	=2	=0
4	1 1 1 1 1 1 | 1	=2	=0	=0
5	1 1 1 1 1 1 | 1	=4	=2	=2
6	1 1 1 1 1 1 | 1	=6	=4	=4

Swap

Byzantine Adversaries Resiliency

- Odd N , N=7

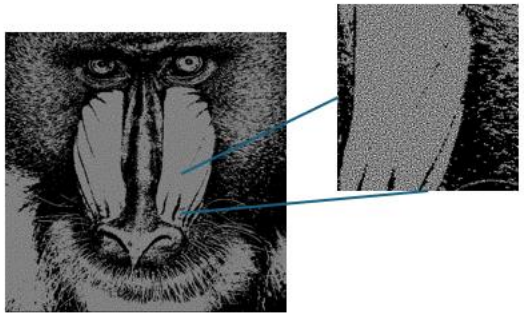
Security Model Results

- Honest-but-curious adversaries - $d \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$
- Byzantine adversaries - $b < \left\lceil \frac{n}{4} \right\rceil - 1, for\ n > 6$

VES Results Comparison

Original Image

Perfectly Recovered Original Image with Waves Interference VES



Grey Recovered Original Image with Naor and Shamir VES

Conclusions and Future Directions

- Collaborative Secure Images Matching
- Grey scale and color images support

Thank You

Alex Fok
alexfok@post.bgu.ac.il