Visual Cryptography

Prepared By:
Dharmendra Kumar
Mentor:
Prof. Malay Ananda Dutta

Overview

- *Introduction*
- *Prensentation work*
- *Conclusion*
- *References*

Introduction

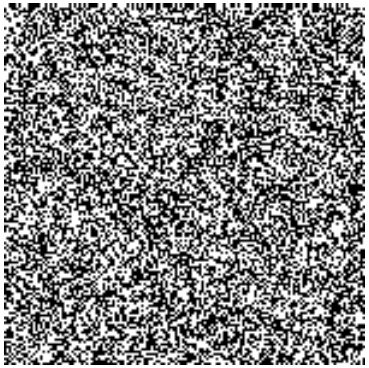
- Visual cryptography (VC) was introduced by Moni Naor and Adi Shamir at *EUROCRYPT 1994*.
- **Visual cryptography** is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that may or may not require a computer.
- It is used to encrypt written material (printed text, handwritten notes, pictures, etc) in a perfectly secure way.
- The decoding is done by the human visual system directly, without any computation cost.

k out of ***n*** sharing problem

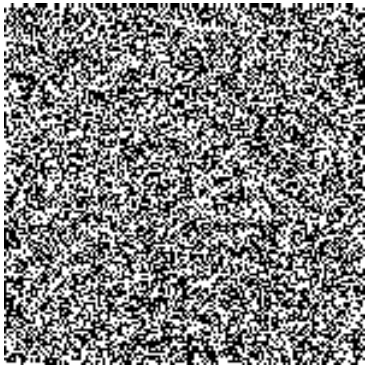
- *k* out of *n* sharing problem
- For a set P of n participants, a secret image S is encoded into n shadow images called shares (shadows), where each participant in P receives one share.
- The original message is visible if any k or more of them are stacked together, but totally invisible if fewer than k transparencies are stacked together.

k out of k example (k=n,n=3)

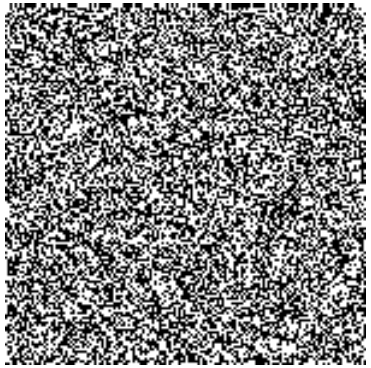
Original



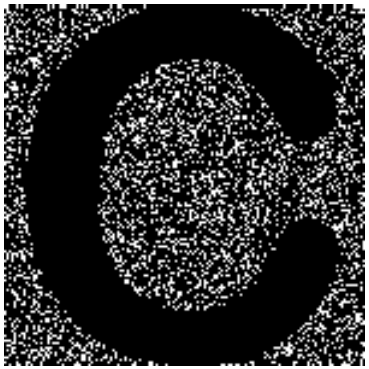
Share



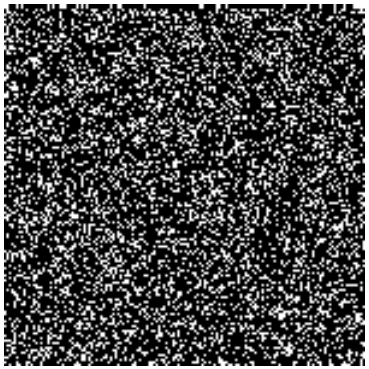
Share



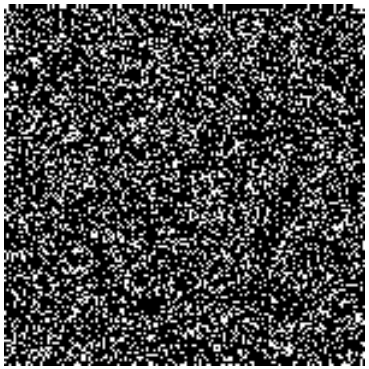
Share



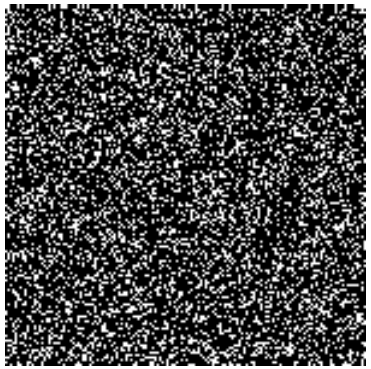
Share #1+#2+#3



Share #1+#2



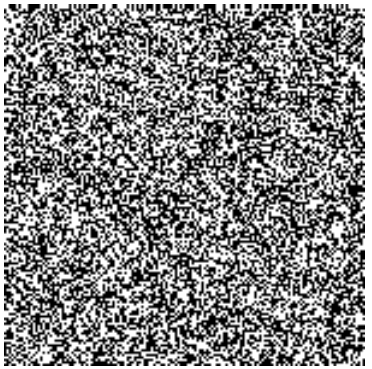
Share #2+#3



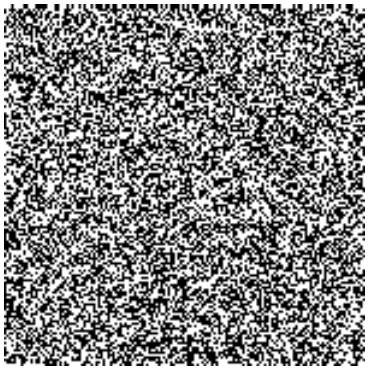
Share #1+ #3

k out of ***n example (k=3,n=4)***

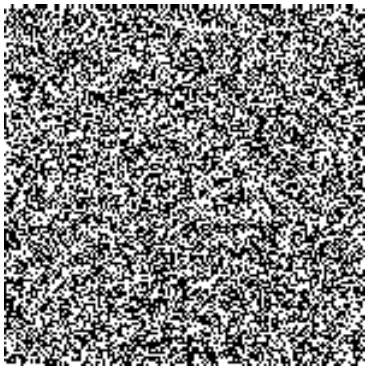
Original



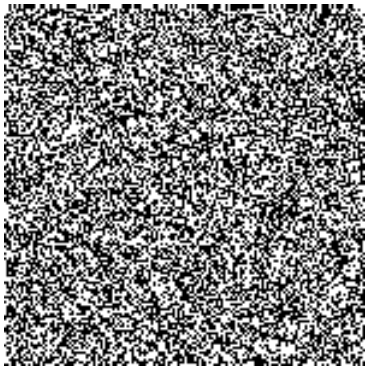
Share 1



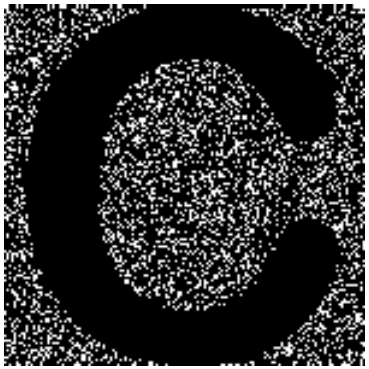
Share 2



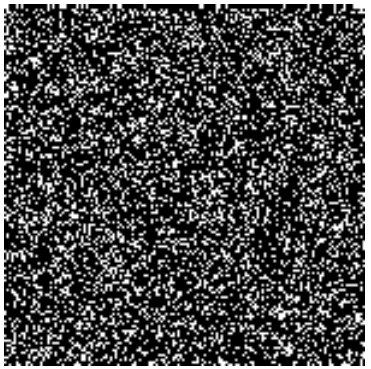
Share 3



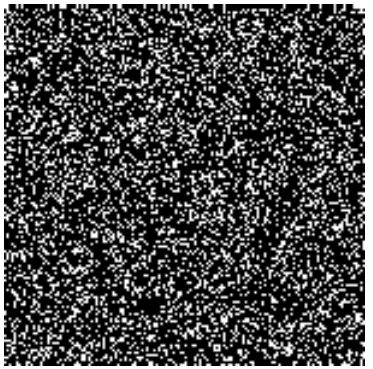
Share 4



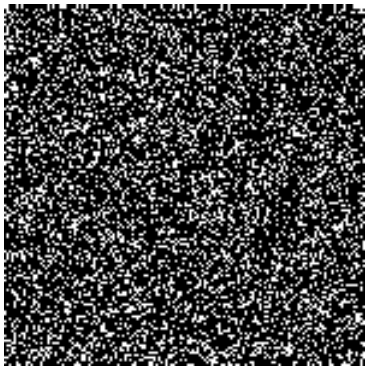
Share 1+2+3



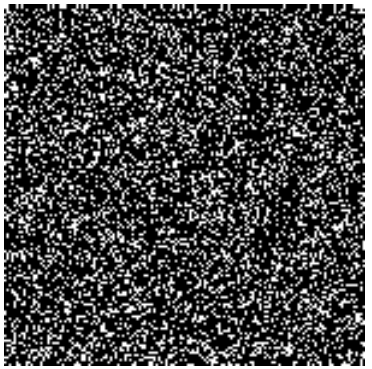
Share 1+2



Share 2+3



Share 4+ 3



Share 1+ 4

General ***k*** out of ***k*** Scheme

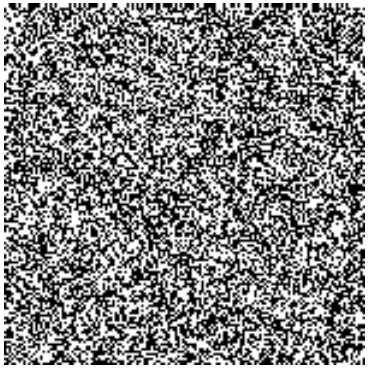
- In k out of k, the image is visible only if a the shares are stacked together.
- If any share in k is lost, and remaining shares are stacked together, it will not form the image.

- Thus, in k out of k, all the shares are important

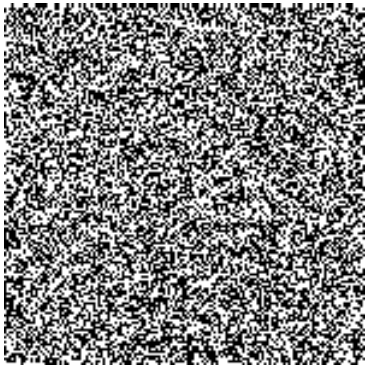
  to construct the image

k out of k example (k=n,n=3)

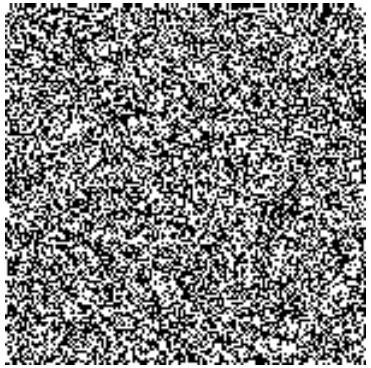
Original



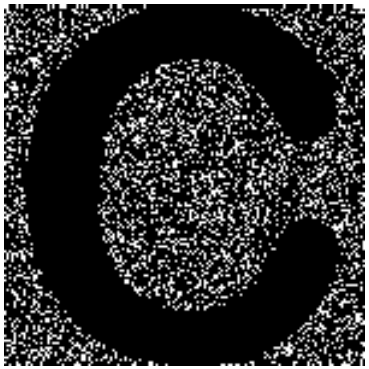
Share



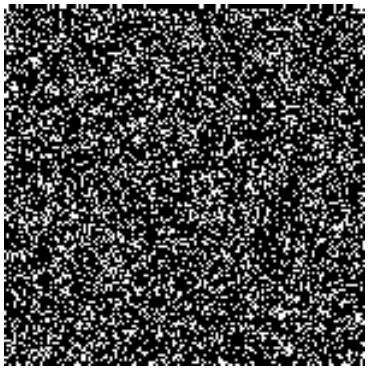
Share



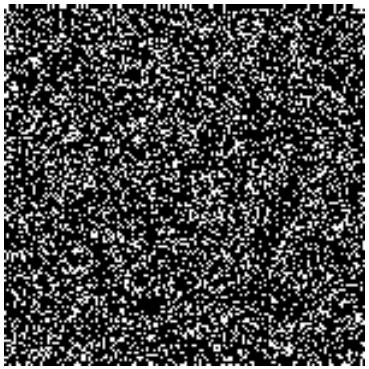
Share



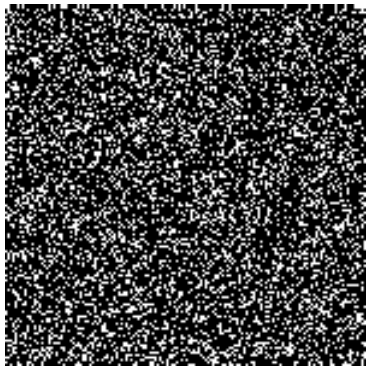
Share #1+#2+#3



Share #1+#2



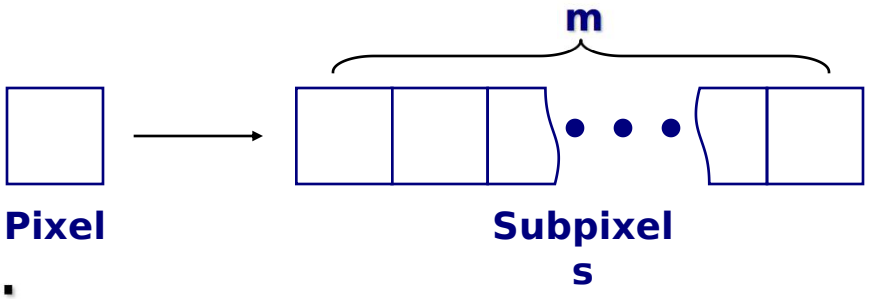
Share #2+#3



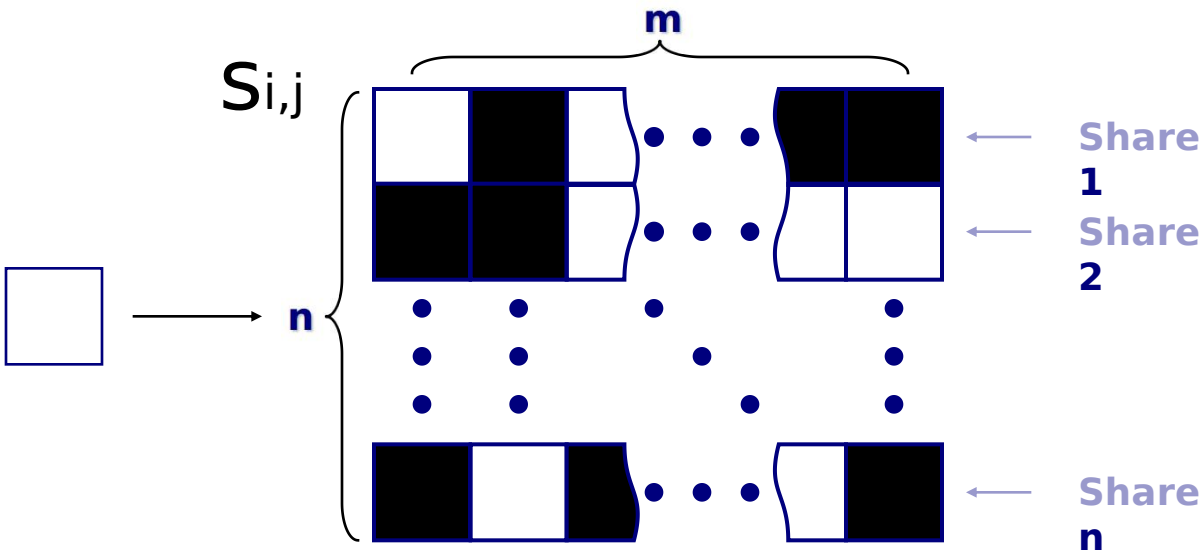
Share #1+ #3

Model

- Pixels are split:



- n shares per pixel:



- Each pixel of image ‘I’ is represented by ‘m’ (m =2) sub pixels in each of the ‘n’ (n=2 in our case) shared images.
- The resulting structure of each shared image is described by Boolean matrix ‘S’
- 1 pixel represented by $n \times m$ Boolean matrix $S = [s_{ij}]$, $s_{ij} = 1$ iff jth sub-pixel in the ith transparency is black

2 out of 2 Scheme (2 subpixels)

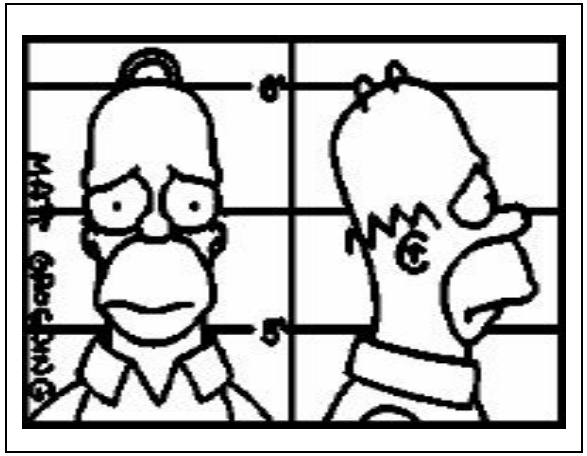
- Black and white image: each pixel divided in 2 sub-pixels
- Randomly choose between black and white.
- Share white pixel: randomly choose one matrix in C 0
- Share black pixel: randomly choose one matrix in C 1

2 out of 2 Scheme (2 subpixels)

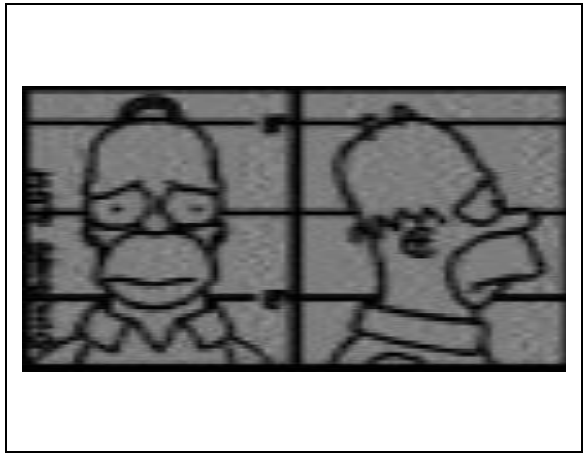
Pixel		Share 1	Share 2	Result
	P = ½			
	P = ½			
	P = ½			
	P = ½			

2 out of 2 Scheme (2 subpixels)

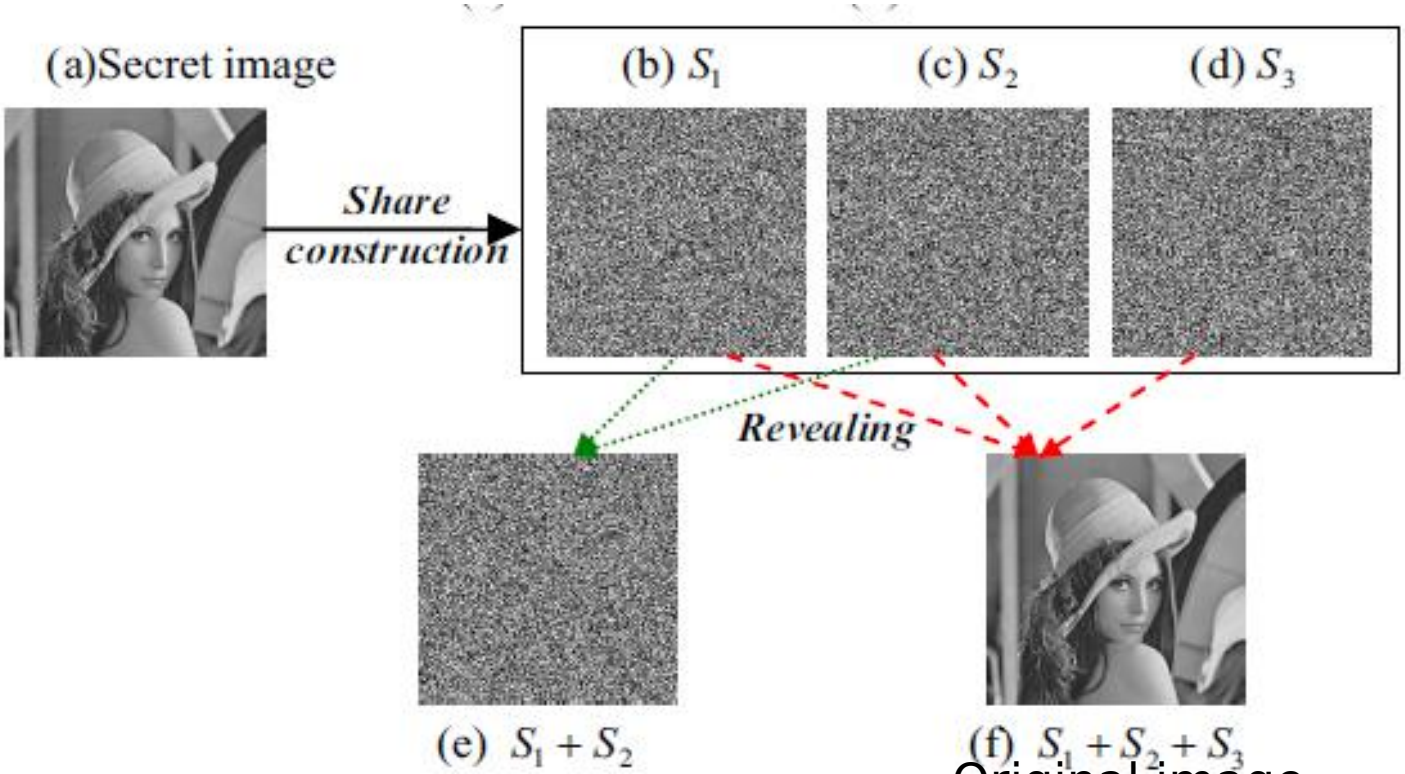
- The two subpixels per pixel variant can distort the aspect ratio of the original image



+



3 out of 3 Scheme Example



(3, 3) secret image sharing scheme for grayscale secret image.

Future Use and Applications

- Remote Electronic Voting
- Anti-Spam Bot Safeguard
- Banking Customer Identification
- Message Concealment
- Key Management

Conclusion

- Shares can be difficult to align (it helps to have fat pixels, but that reduces quality),
- Contrasts declines rapidly with the number of shares.
- It is not wrong to tell that no information can be constructed from a single share.
- The method enables a tight security to the secret message

References

1.M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYFT'94, LNCS, vol. 950, pp. 1-12,1995

2.John Blesswin, Rema, Jenifer Josel, “ Recovering Secret Image in Visual Cryptography”, Karunya University,538

3.S. Cimato, R. De Prisco, and A. De Santis, ‘Probabilistic visual cryptography schemes’. The Computer Journal, 49(1):97,107,

December 2005