CRYPTOGRAPHY

PRATIKSHA PATIL

CONTENTS

- Introduction
- Need of Cryptography
- Types of Attacks
- Techniques of Cryptography
- Encryption Algorithm
  - Symmetric
  - Asymmetric
- Digital Signature
- Visual cryptography

INTRODUCTION

- What is Cryptography?

  - “Hidden Writing”
  - Mainly used to protect Information.

NEED OF ENCRYPTION

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation
- Access Control
- Availability

TYPES OF ATTACKS

- A General View:

1. Criminal attacks
2. Publicity attacks

- A Technical View:

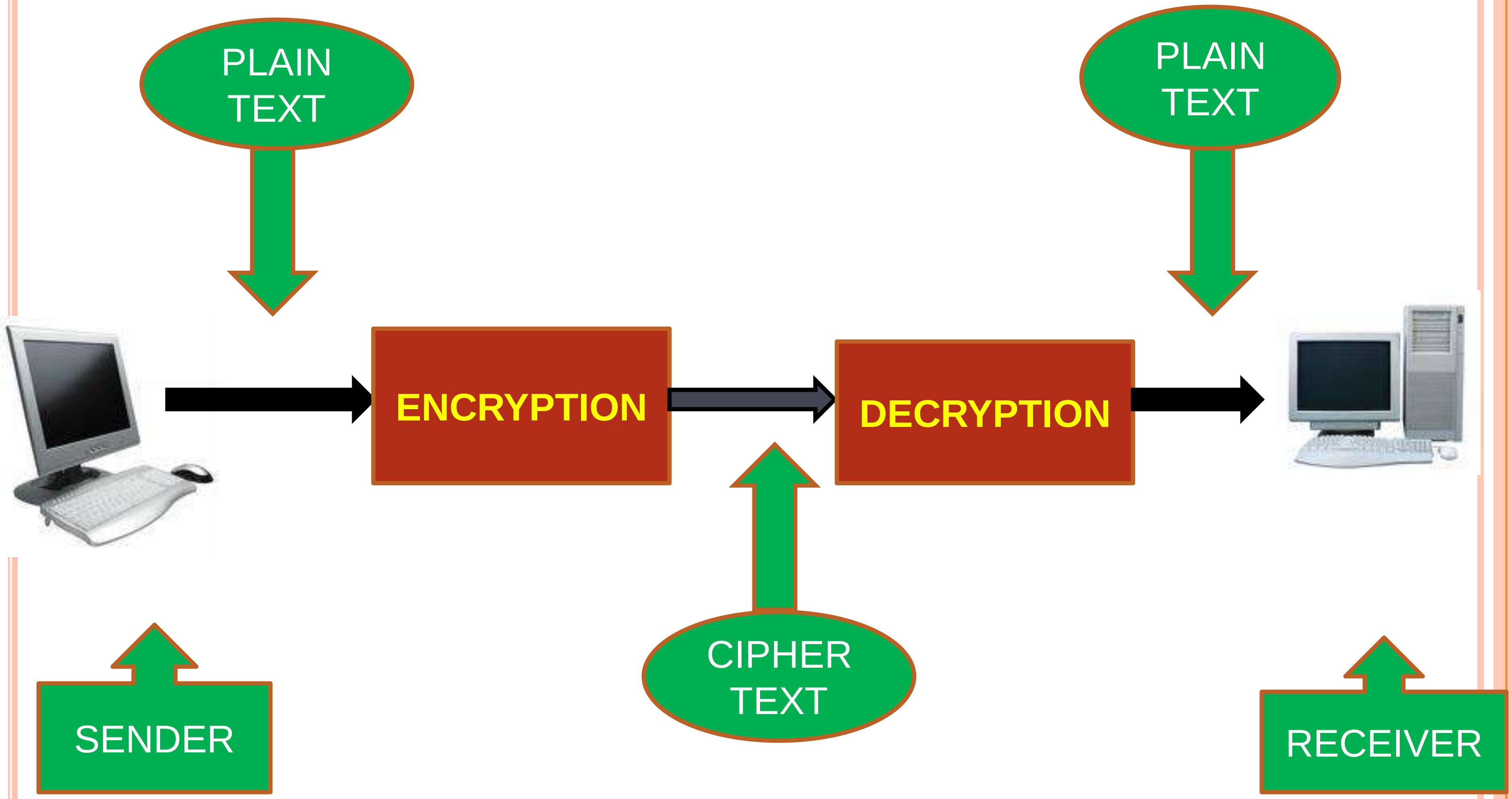
1. Passive attacks
2. Modification
3. Fabrication

- A Practical Side of Attacks:

1. Application level
2. Network level

- Programs that Attack:

1. Virus(infects)
2. Worm (replicates)
3. Trojan (hidden)
4. Applets and Active X controls (downloadable)



PLAIN TEXT

PLAIN TEXT

ENCRYPTION

DECRYPTION

CIPHER TEXT

SENDER

RECEIVER

BASIC BLOCK DIAGRAM

Basic Terminologies

- Encryption
  - Encryption is the process of encoding a message so that its meaning is not obvious
- Decryption
  - Decryption is the reverse process, transforming an encrypted message back into its normal, original form
- Cryptosystem
  - A system for encryption and decryption is called a cryptosystem.

Basic Terminologies

- Plaintext
- Cipher text
- Key –
  - key refers to a sequence of symbols or a numerical value used by an algorithm to alter information & making that information secure

- Encryption algorithm
  - The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the cipher text.
- Cryptanalysis
  - Cryptanalysis is an attempt to break the cipher text.

Techniques of Cryptography

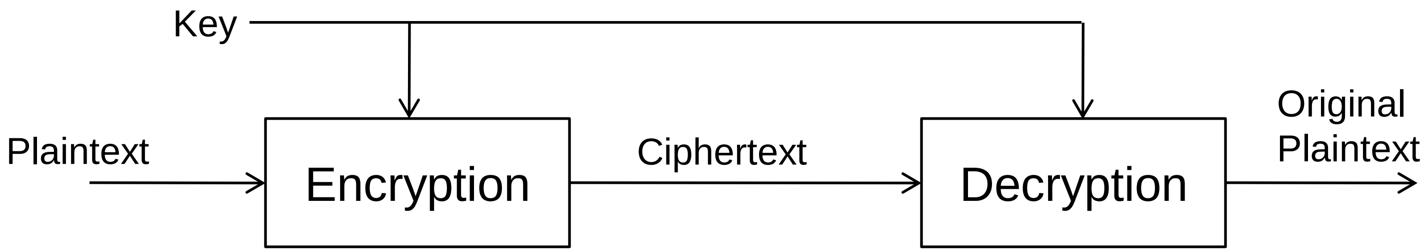
- Substitution Technique
  - Caesar Cipher
  - Monoalphabetic Cipher
  - Playfair Cipher
  - Polyalphabetic Cipher
- Transposition Technique
  - Rail Fence Technique
  - Vernam Cipher(One -time Pads)
  - Simple Columnar Cipher

Encryption Algorithm

- Symmetric
  - Same key for encryption and decryption
  - Key distribution problem
- Asymmetric
  - Key pairs for encryption and decryption
  - Public and private keys

SYMMETRIC ALGORITHM

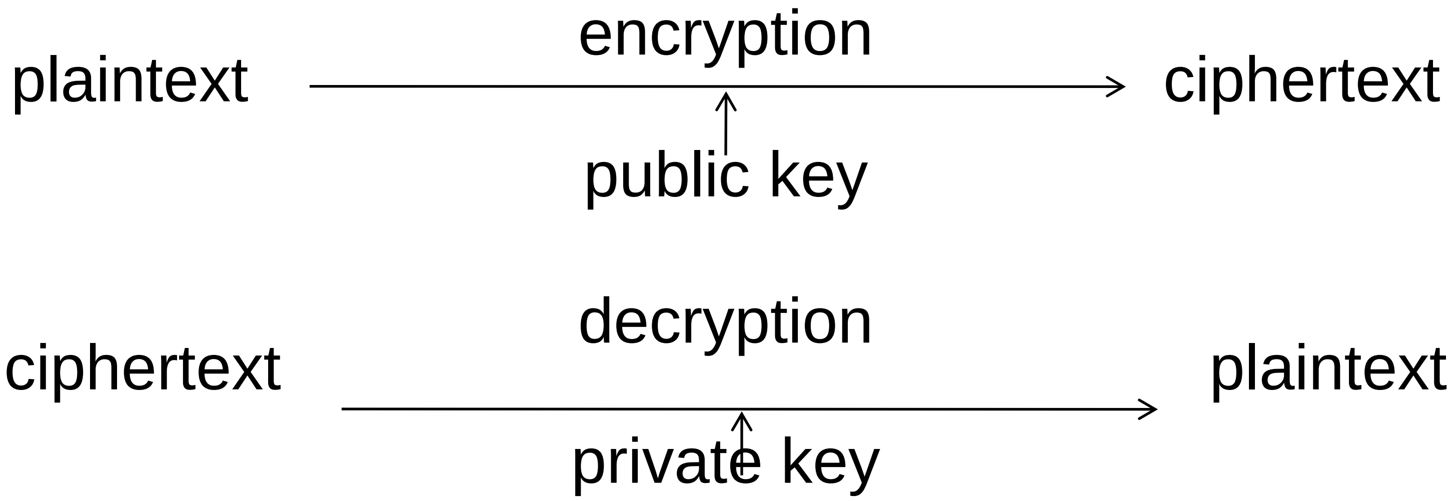
- It is also called as Secret Key Cryptography
  - Single key used for both encrypt & decrypt
  - Key must be known to both the parties



Symmetric Cryptosystem

Asymmetric Algorithm

- Private keys are used for decrypting.
- Public keys are used for encrypting



plaintext

encryption

ciphertext

public key

ciphertext

decryption

plaintext

private key

SYMMETRIC ALGORITHM

- Data Encryption Standard (DES):

  56 bits key

- Advance Encryption Standard (AES):

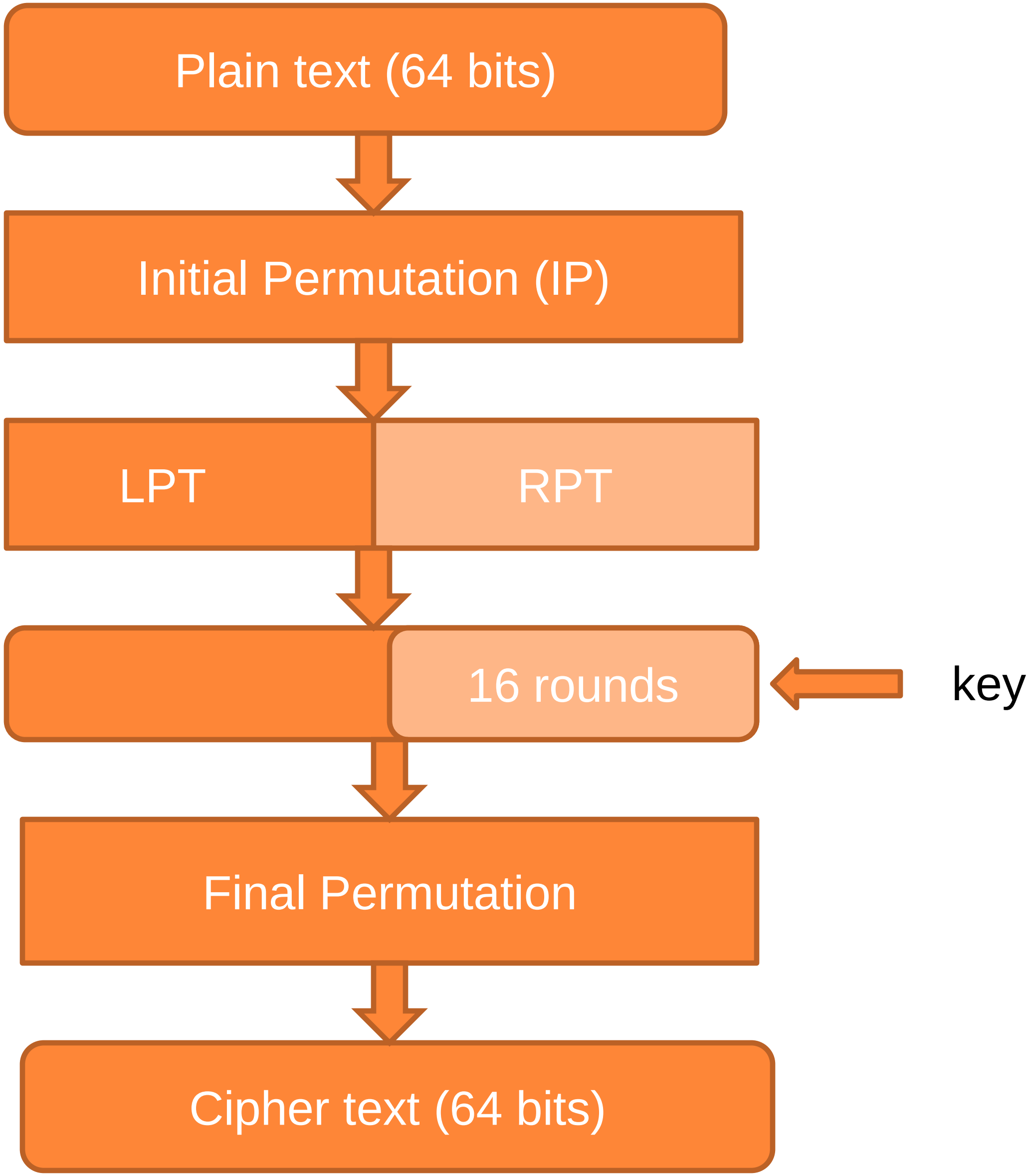
  128, 192 or 256 bits key

- International Data Encryption Algorithm(IDEA):

  128 bits key

DATA ENCRYPTION STANDARD

- Developed by IBM and it is known as the Data Encryption Standard
- It is also known as Data Encryption Algorithm
- The DES algorithm is a careful and complex combination of two fundamental building blocks of encryption:
  - Substitution and
  - Transposition
- DES uses only standard arithmetic and logical operations on numbers up to 64 bits long

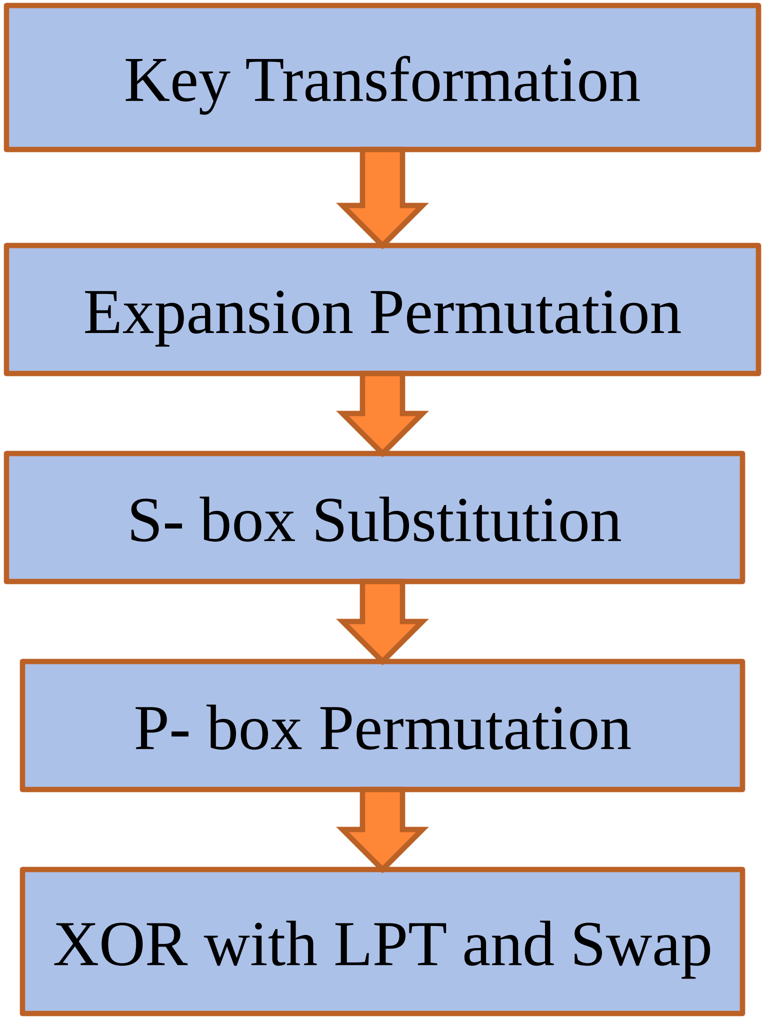


BROAD LEVEL STEPS IN DES

DATA ENCRYPTION STANDARD

- 1st 64 bit plain text is handed over to initial permutation function.
- IP is performed over the plain text.
- IP produces two halves of the permuted blocks left plain text (LPT) & right plain text (RPT).
- Now LPT & RPT goes 16 rounds of encryption process, each with its own key.
- Now LPT & RPT are rejoined and FINAL PERMUTATION (FP) is performed on the combined block.
- The result is 64 bit cipher text.

DETAILS OF ONE ROUND IN DES



Key Transformation

64-56-
48BITS

Expansion Permutation

32-48BITS

S- box Substitution

48-32BITS

P- box Permutation

XOR with LPT and Swap

RPT

ADVANTAGES OF DES:

- DES is also an ANSI and ISO standard - anybody can learn the details and implement it.
- Hard to crack.

DISADVANTAGES OF DES:

- Software implementations of DES are slow.

Asymmetric Algorithm

- Rivest Shamir Adleman (RSA) Encryption:

  Based on factoring the product of large prime numbers.

- Knapsack Algorithm:

  If M1,M2…., Mn are given values & S is the sum,
  S=b1M1+b2M2….+bnMn
  where, bi can be 0 or 1

RSA

- It is named after its three inventors **R**ivest **S**hamir and **A**dleman
- This algorithm was introduced in 1978 and to date remains secure.
- RSA has been the subject of extensive cryptanalysis, and no serious flaws have yet been found.
- The encryption algorithm is based on the underlying problem of factoring large numbers.

Generating Public and Private Keys

1. pick two prime numbers, we'll pick p = 3 and q = 11
2. calculate n = p * q = 3 * 11 = 33
   calculate z = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20
3. choose a prime number k, such that k is co-prime to z, i.e, z is not divisible by k. We have several choices for k: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5). Let's pick k=7
4. So, the numbers n = 33 and k = 7 become the Server's public key.

1. Now, still done in advance of any transmission, the Server has to calculate it's secret key. Here is how.
2. k * j = 1 (mod z)
3. 7 * j = 1 (mod 20)
4. (7 * j) / 20 = ? with the remainder of 1
5. 21 / 20 gives "something" with the remainder of 1. So, 7 * j = 21, and j = 3. This is our secret key.

Encrypting the message

Here is the encryption math that Browser executes.

P ^ k = E (mod n)

P is the Plain message we want to encrypt

n and k are Server's public key

E is our Encrypted message we want to generate

After plugging in the values, this equation is solved as follows:

14 ^ 7 = E (mod 33)

This equation says: raise 14 to the power of 7, divide this by 33, giving the remainder of E.

105413504 / 33 = 3194348.606

3194348 * 33 = 10541348

E = 105413504 - 10541348 = 20

- So, our Encrypted message is E=20. This is now the value that the Browser is going to send to the Server. When the Server receives this message, it then proceeds to Decrypt it, as follows.

Decrypting the Message

Here is the decryption math the Server executes to recover the original Plain text message which the Browser started with.

$E ^ j = P (\text{mod } n)$

E is the Encrypted message just received

j is the Server's secret key

P is the Plain message we are trying to recover

n is Server's public key

After plugging in the values:

$20 ^ 3 = P (\text{mod } 33)$

8000 / 33 = ? with the remainder of P. So to calculate this remainder:

8000 / 33 = 242.424242...

242 * 33 = 7986

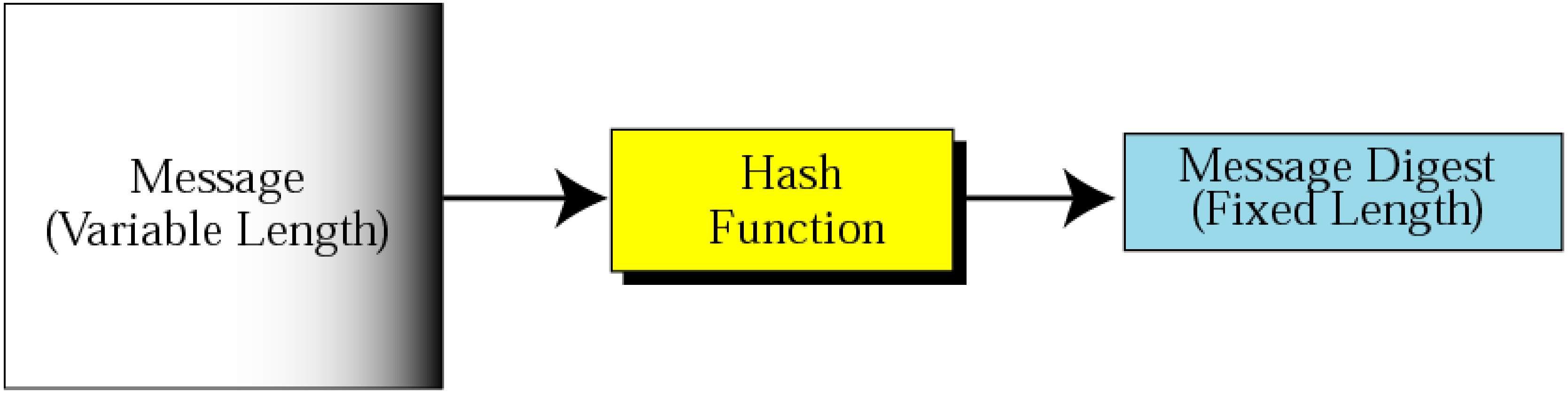
P = 8000 - 7986 = 14, which is exactly the Plain text message that the Browser started with!

Digital signature

- When an author signs a document, it cannot be changed.

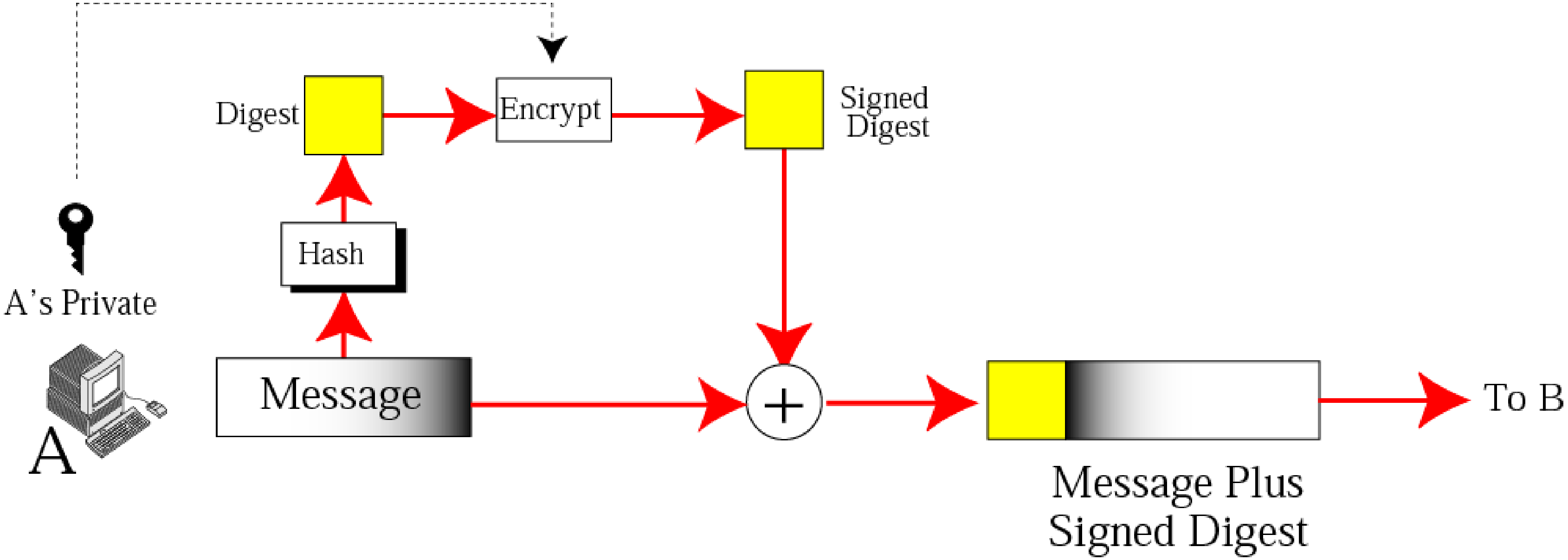
- When you send a document electronically, you can also sign it.

Signing the digest

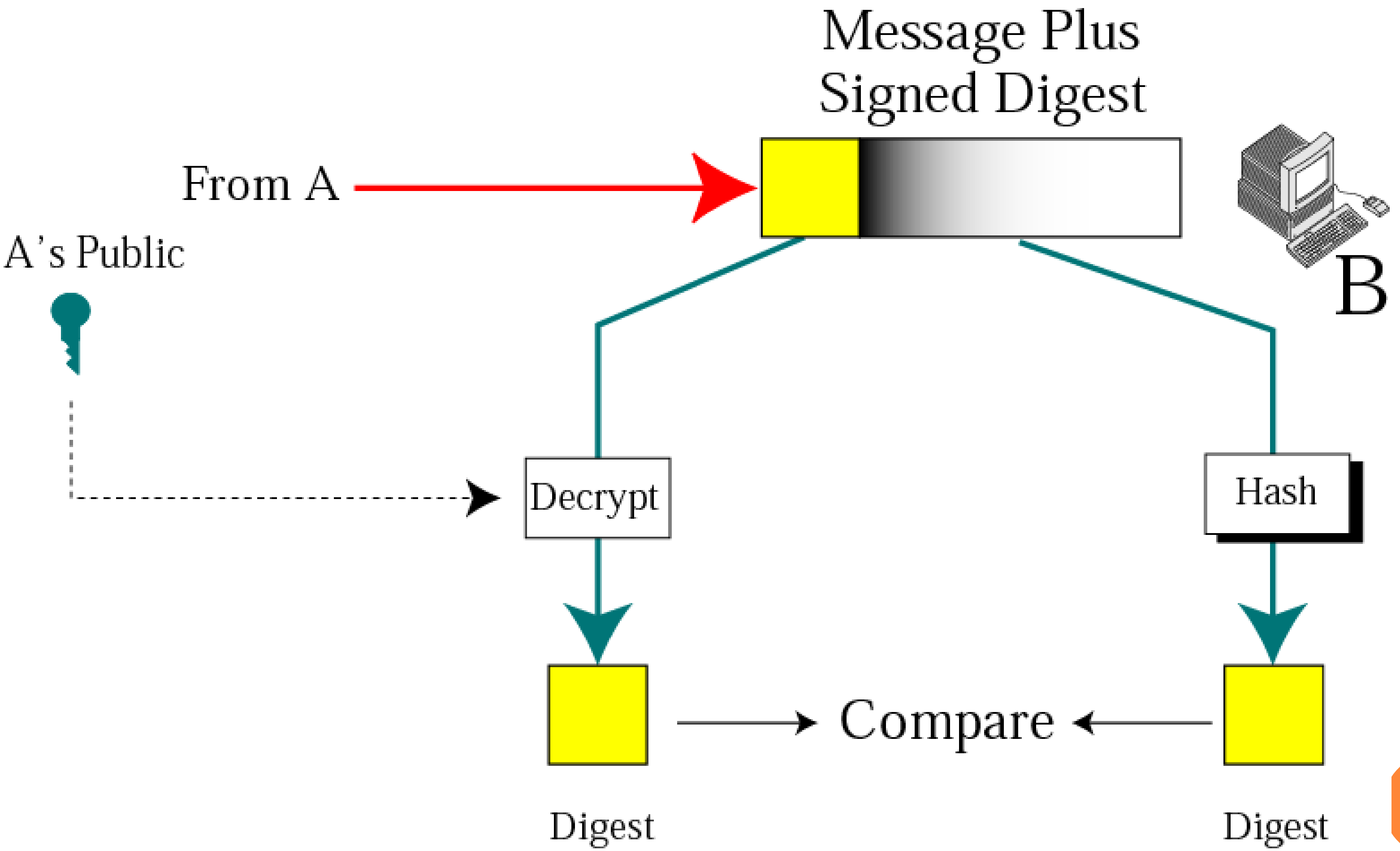


- The two most common hash functions are:
  - Message digest 5 (MD5)
  - Secure hash algorithm (SHA-1)
- The properties of hash function
  - One-way: the digest can only be created from the message, but not vice versa
  - One-to-one: be very difficult to find two messages that create the same digest.

Sender site


Digest
Encrypt
Signed Digest
Hash
A's Private
Message
A
+
To B
Message Plus Signed Digest

Receiver site



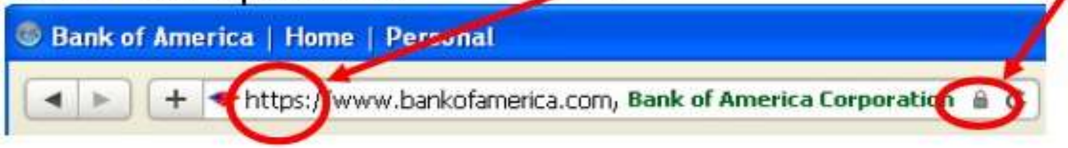
WEB SECURITY

- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable
- have a variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

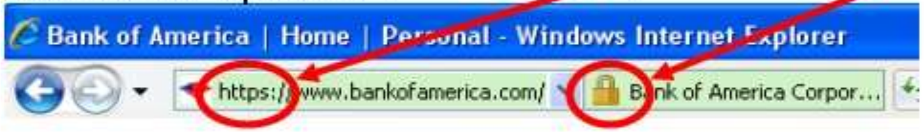
SSL (Secure Socket Layer)

- transport layer security service
- originally developed by Netscape
- uses TCP to provide a reliable end-to-end service

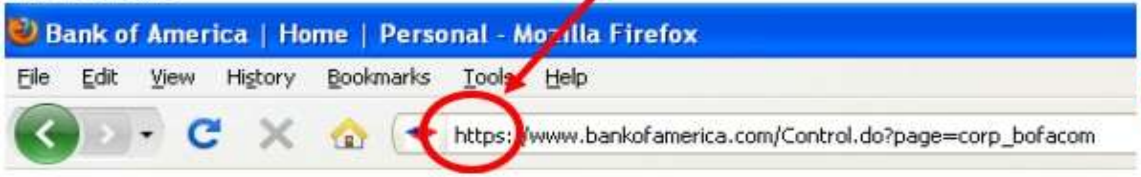
Internet Explorer 8 “https” SSL lock symbol

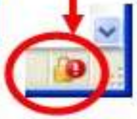

Bank of America | Home | Personal
https://www.bankofamerica.com/ Bank of America Corporation

Internet Explorer 7 “https” SSL lock symbol


Bank of America | Home | Personal - Windows Internet Explorer
https://www.bankofamerica.com/
Bank of America Corpor...

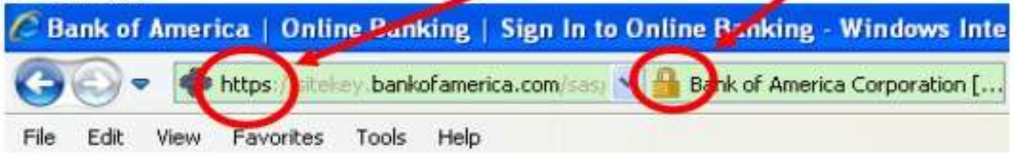
Firefox “https” SSL lock symbol


Bank of America | Home | Personal - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
https://www.bankofamerica.com/Control.do?page=corp_bofacom

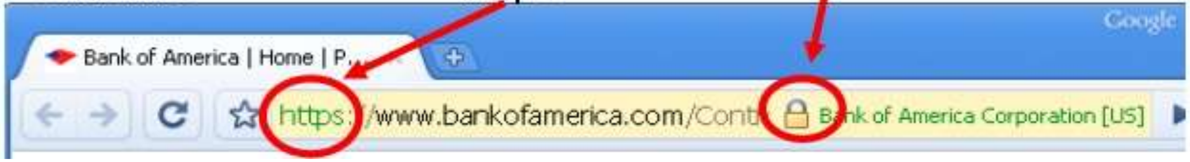


Firefox
Lower right corner

Safari “https” SSL lock symbol


Bank of America | Online Banking | Sign In to Online Banking - Windows Inte
https://sitekey.bankofamerica.com/sas/
Bank of America Corporation [...
File
Edit
View
Favorites
Tools
Help

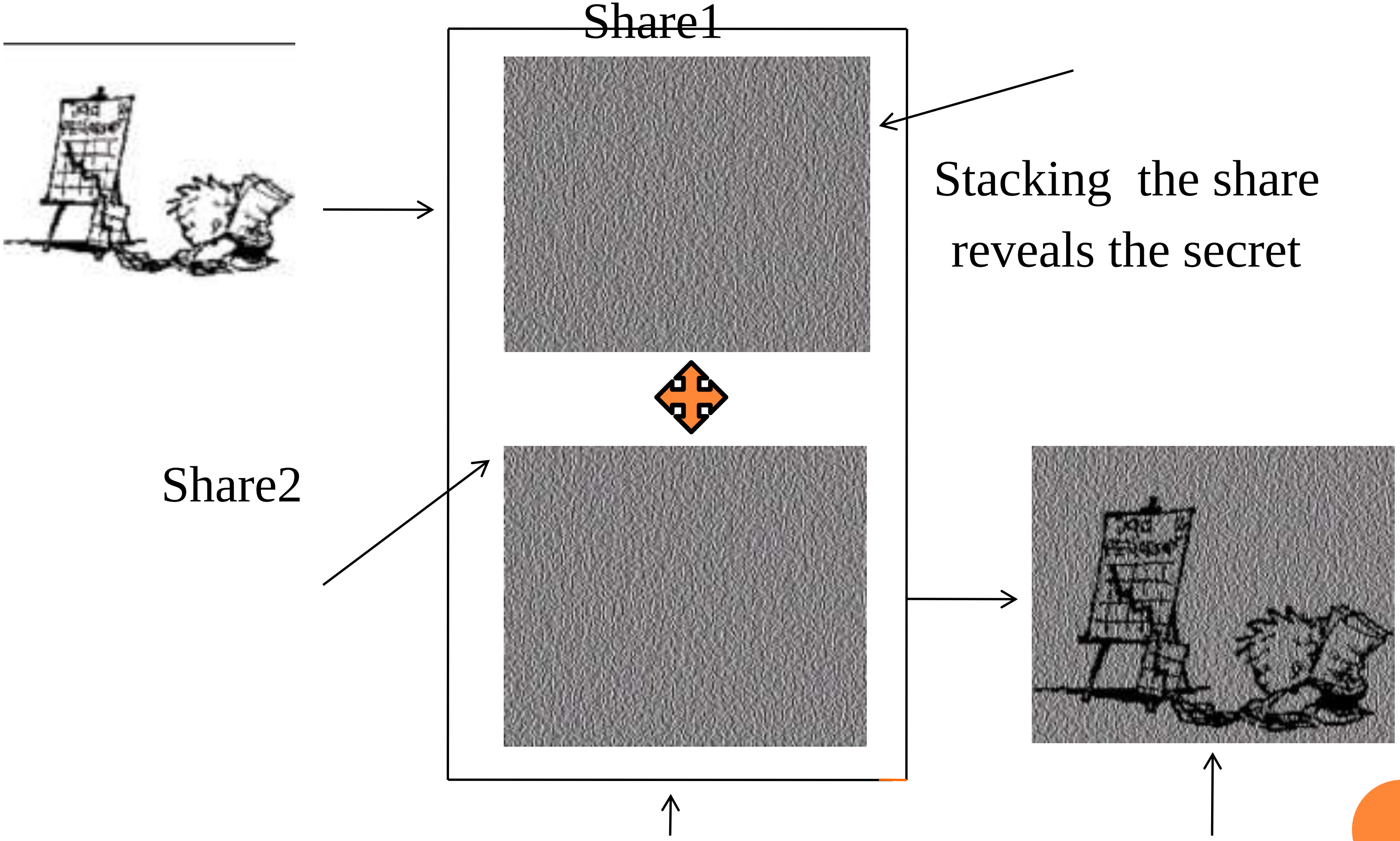
Chrome “https” SSL lock symbol


Google
Bank of America | Home | P...
https://www.bankofamerica.com/Cont
Bank of America Corporation [US]

SSL Handshake Protocol

- allows server & client to:
  - authenticate each other
  - to negotiate encryption
  - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish

Overview of Visual Cryptography



Share1

Stacking the share reveals the secret

Share2

Encryption

Decryption

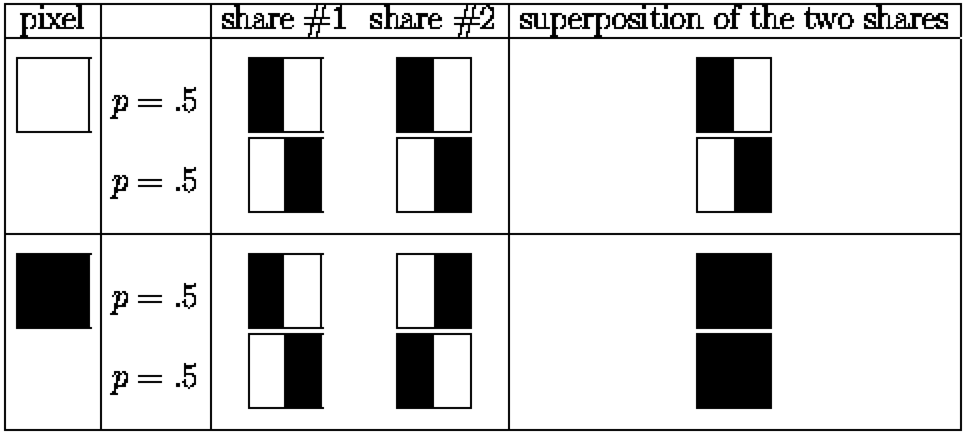
The basis matrices and the collections of the encoding matrices in the conventional (2,2) scheme can be written as:

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

IMPLEMENTATION



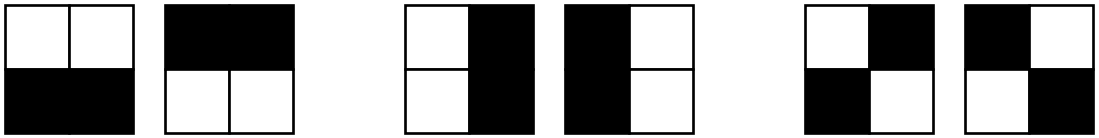
pixel		share #1	share #2	superposition of the two shares
□	$p = .5$	◧	◧	◧
	$p = .5$	◨	◨	◨
■	$p = .5$	◧	◨	■
	$p = .5$	◨	◧	■

FIG 1

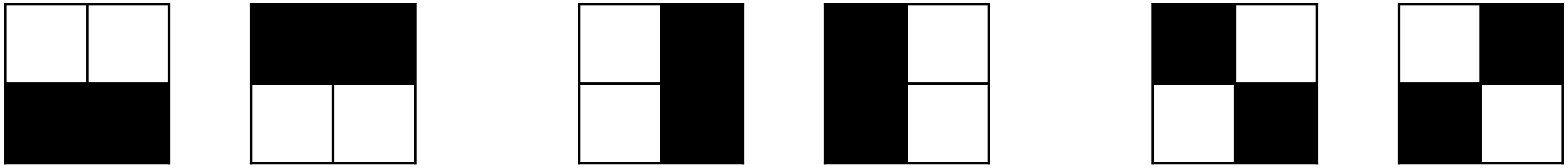
$$C_0 = \left\{ \begin{bmatrix} 01 \\ 01 \end{bmatrix} \begin{bmatrix} 10 \\ 10 \end{bmatrix} \right\} \qquad C_1 = \left\{ \begin{bmatrix} 01 \\ 10 \end{bmatrix} \begin{bmatrix} 10 \\ 01 \end{bmatrix} \right\}$$

2 out of 2 Scheme (4 sub pixels)

- 6 ways to place two black subpixels in the 2 x 2 square



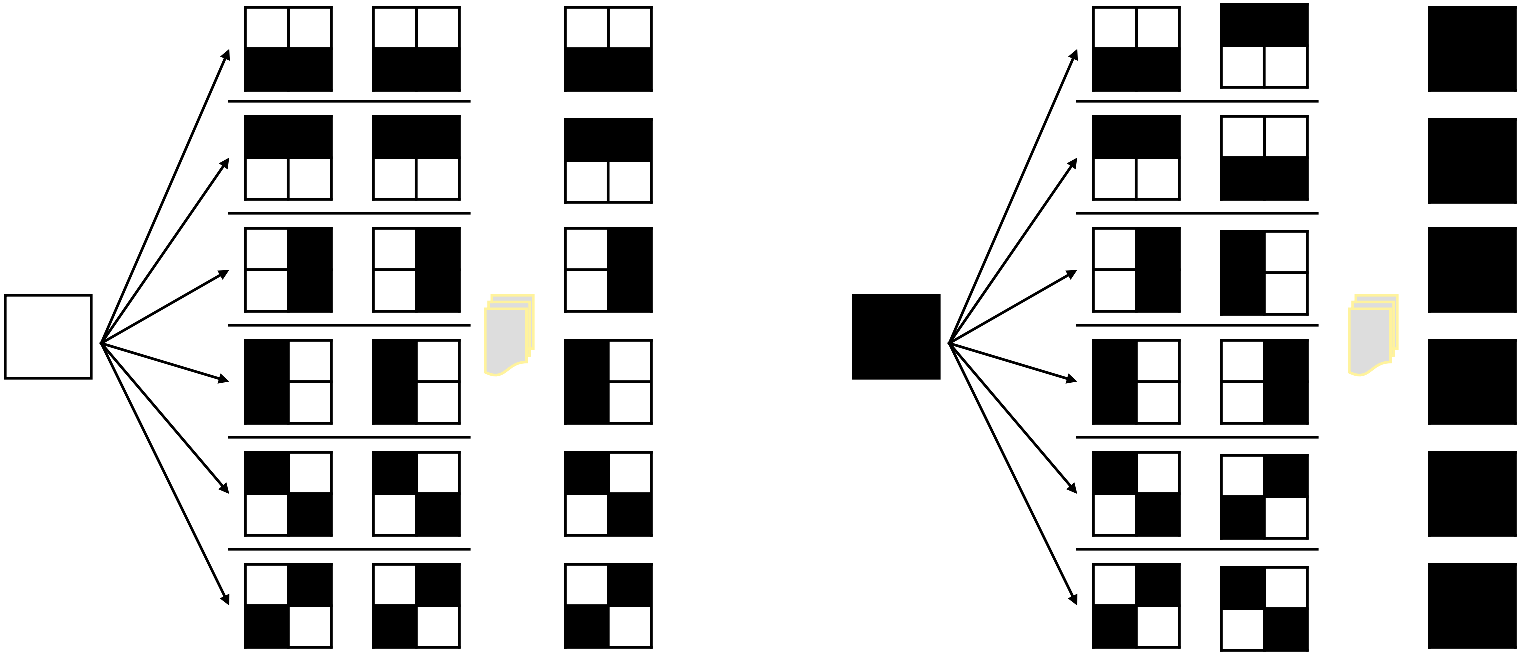
2 out of 2 Scheme (4 subpixels)



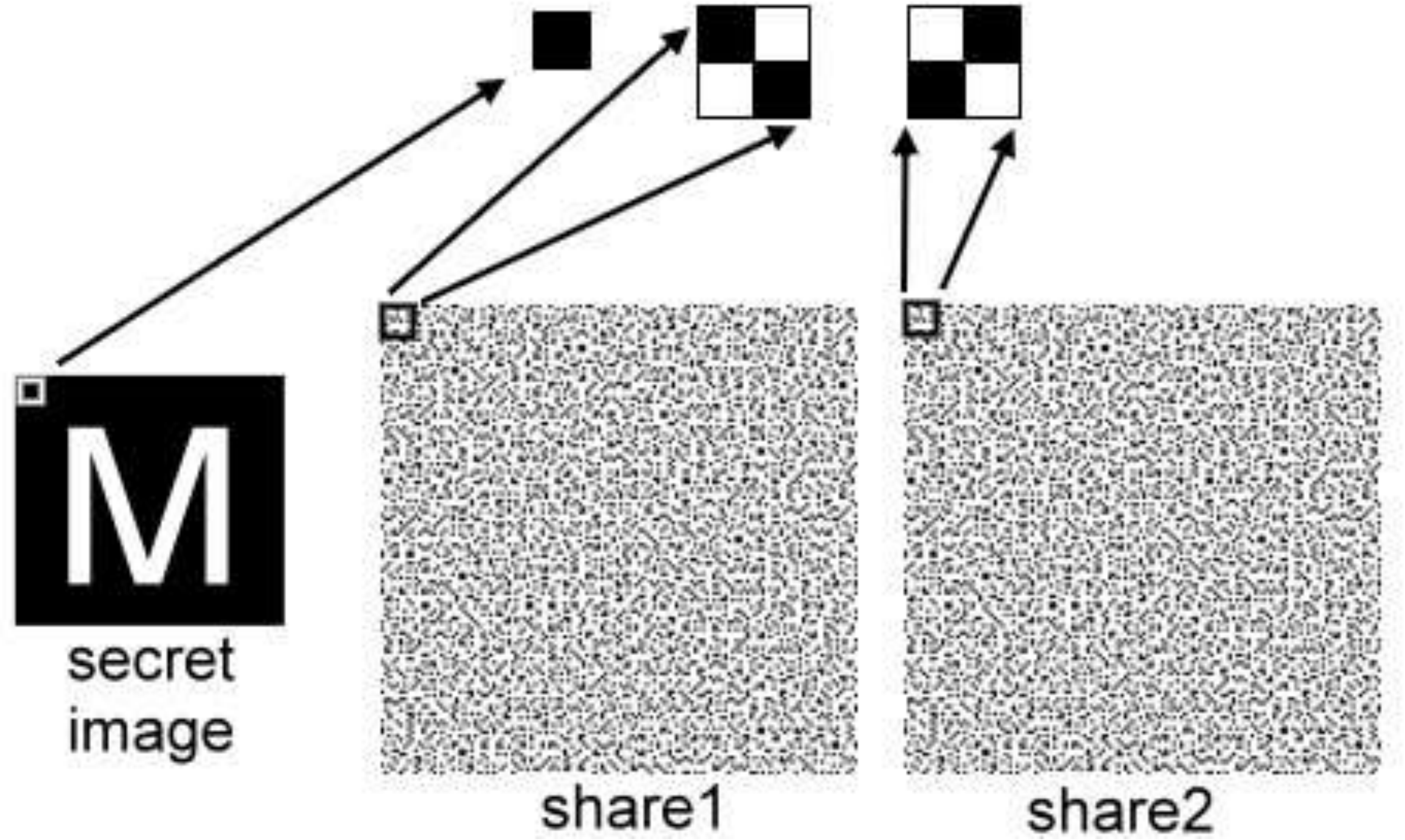
Horizontal shares

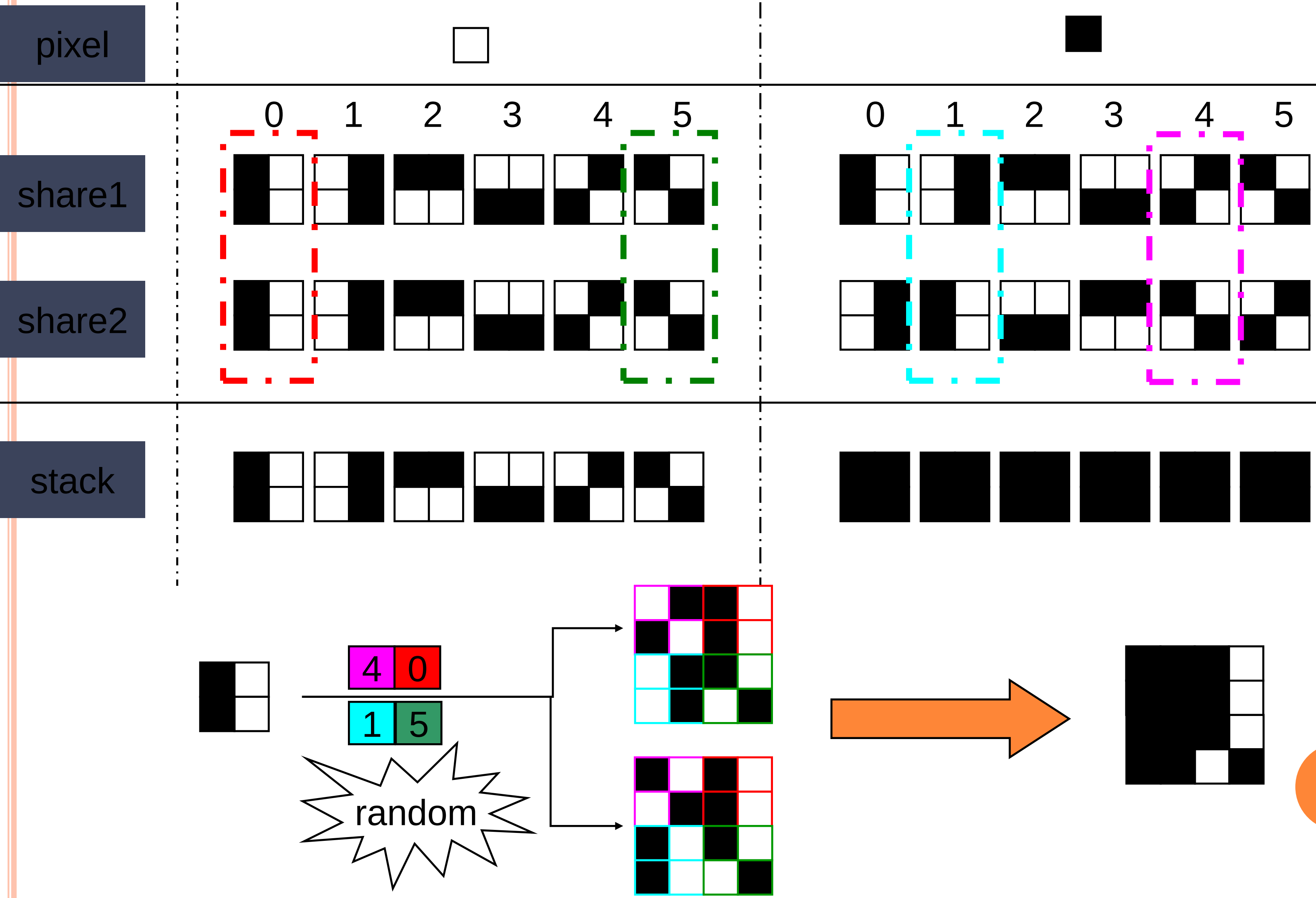
Vertical shares

Diagonal shares



2 out of 2 Scheme (4 sub pixels)





pixel

share1

share2

stack

0 1 2 3 4 5

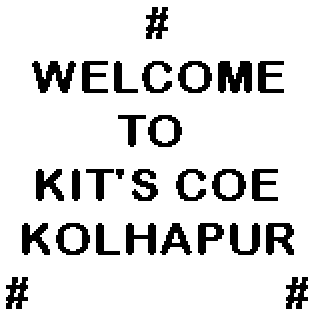
0 1 2 3 4 5

4 0

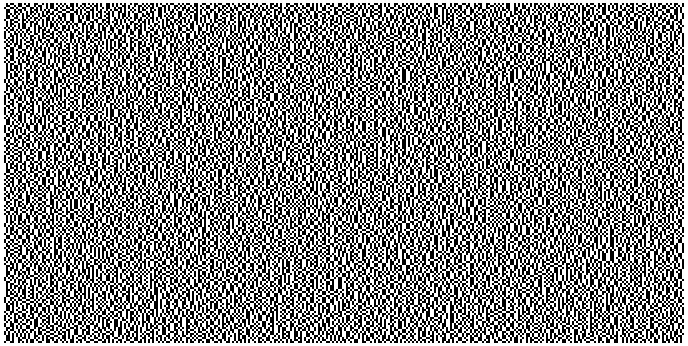
1 5

random

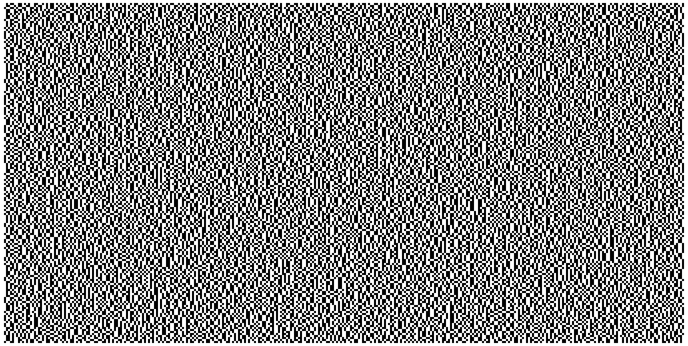
EXAMPLE OF TWO-OUT-OF-TWO VC SCHEME:



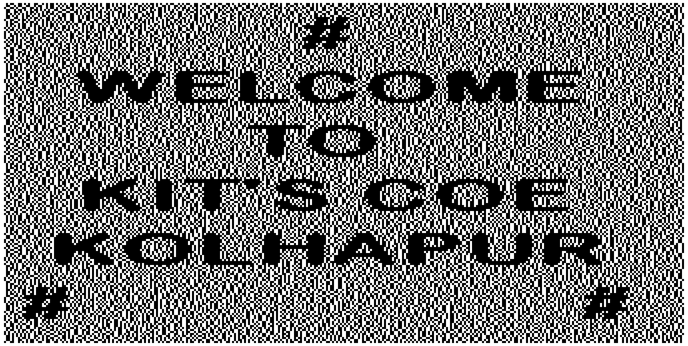
(a)



(b)



(c)

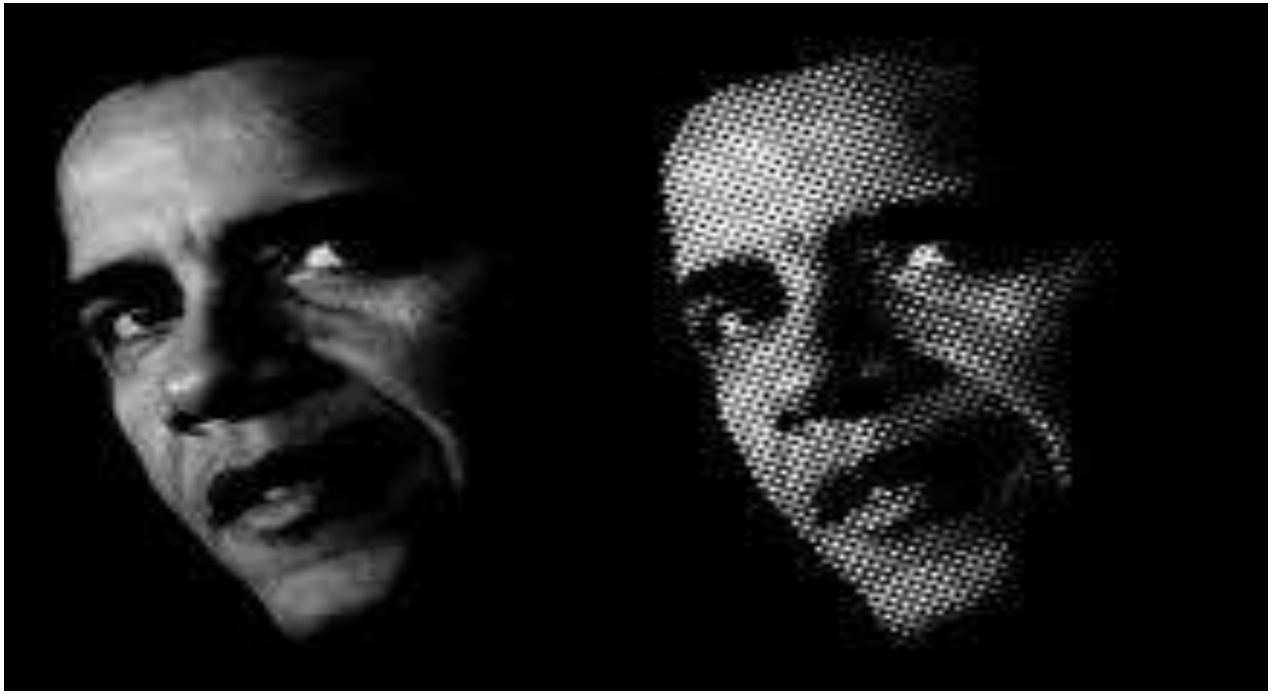


(d)

Halftone Visual Cryptography

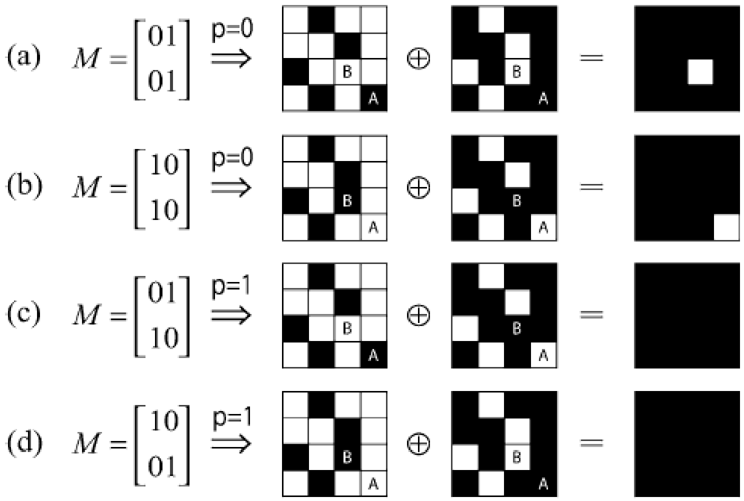
1. The halftoning technique is used to convert the gray-scale image into the binary image.

2. The methods of halftoning that we are going to use are **Error Diffusion** and **Direct Binary Search**.



Background

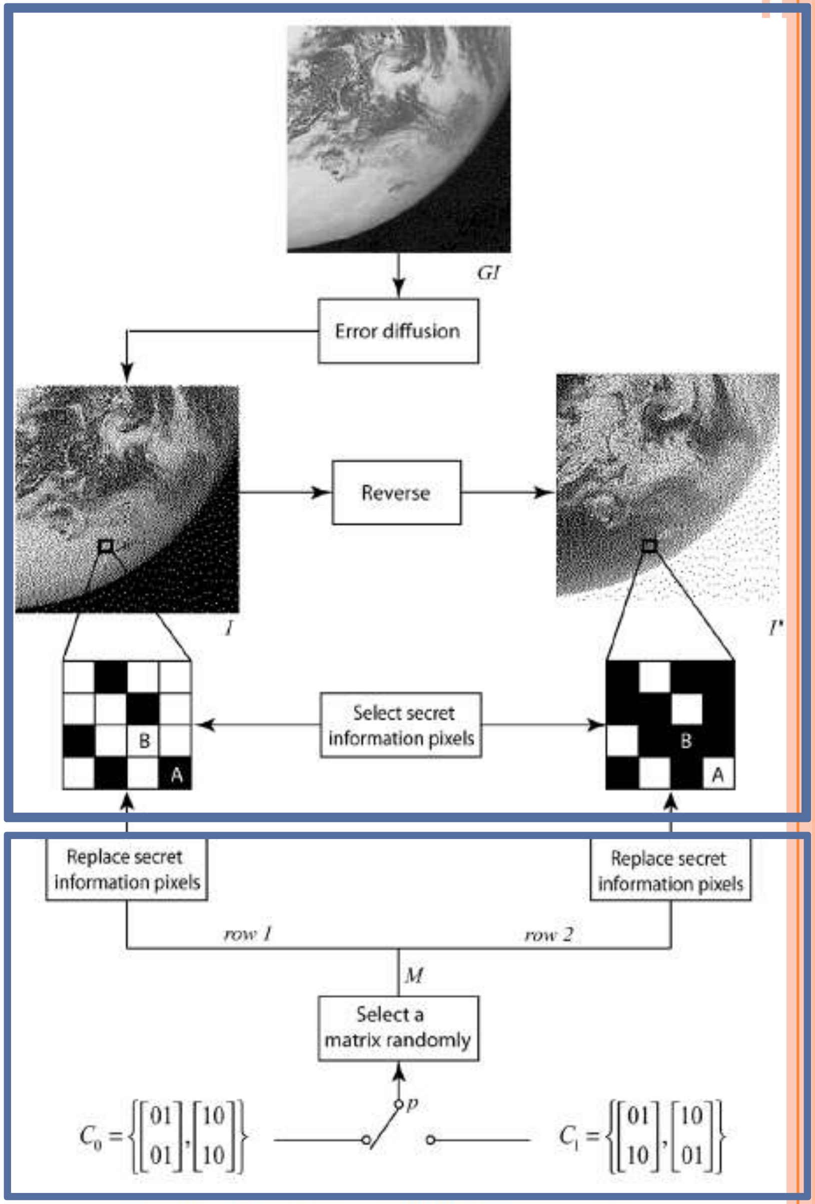
Halftone Visual Cryptography


(a) $M = \begin{bmatrix} 01 \\ 01 \end{bmatrix}$ p=0 ⇒
(b) $M = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$ p=0 ⇒
(c) $M = \begin{bmatrix} 01 \\ 10 \end{bmatrix}$ p=1 ⇒
(d) $M = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$ p=1 ⇒
B
A
⊕
=

⊕ : superimpose two halftone cells

Replacing the secret information pixels with the corresponding subpixels in a matrix M, which is randomly selected as (a), (b) from C_0 if $p = 0$, or (c), (d) from C_1 if $p = 1$. The secret pixel p can be visually decoded by superimposing the two shares.

Distributions of SIPs


GI
Error diffusion
Reverse
I
I'
Select secret information pixels
B
A
Replace secret information pixels
Replace secret information pixels
row 1
row 2
M
Select a matrix randomly
p
$C_0 = \left\{ \begin{bmatrix} 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 10 \\ 10 \end{bmatrix} \right\}$
$C_1 = \left\{ \begin{bmatrix} 01 \\ 10 \end{bmatrix}, \begin{bmatrix} 10 \\ 01 \end{bmatrix} \right\}$

Construction of a two-out-of-two scheme. Cell size is $Q = 4$.

Assign the values of all SIPs

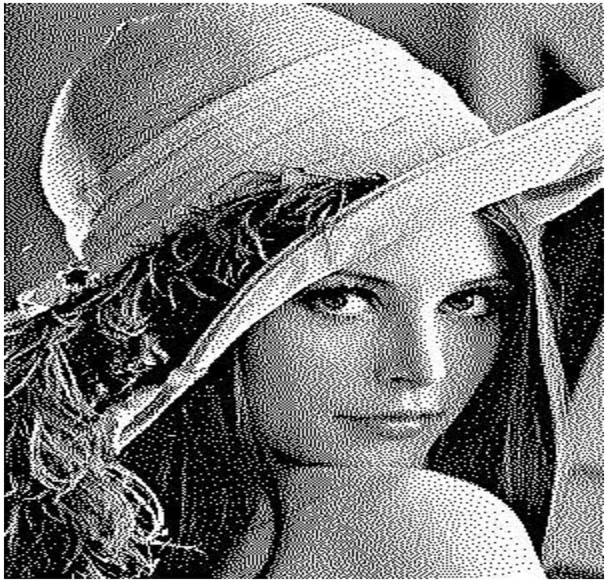
underlying VC scheme

Er

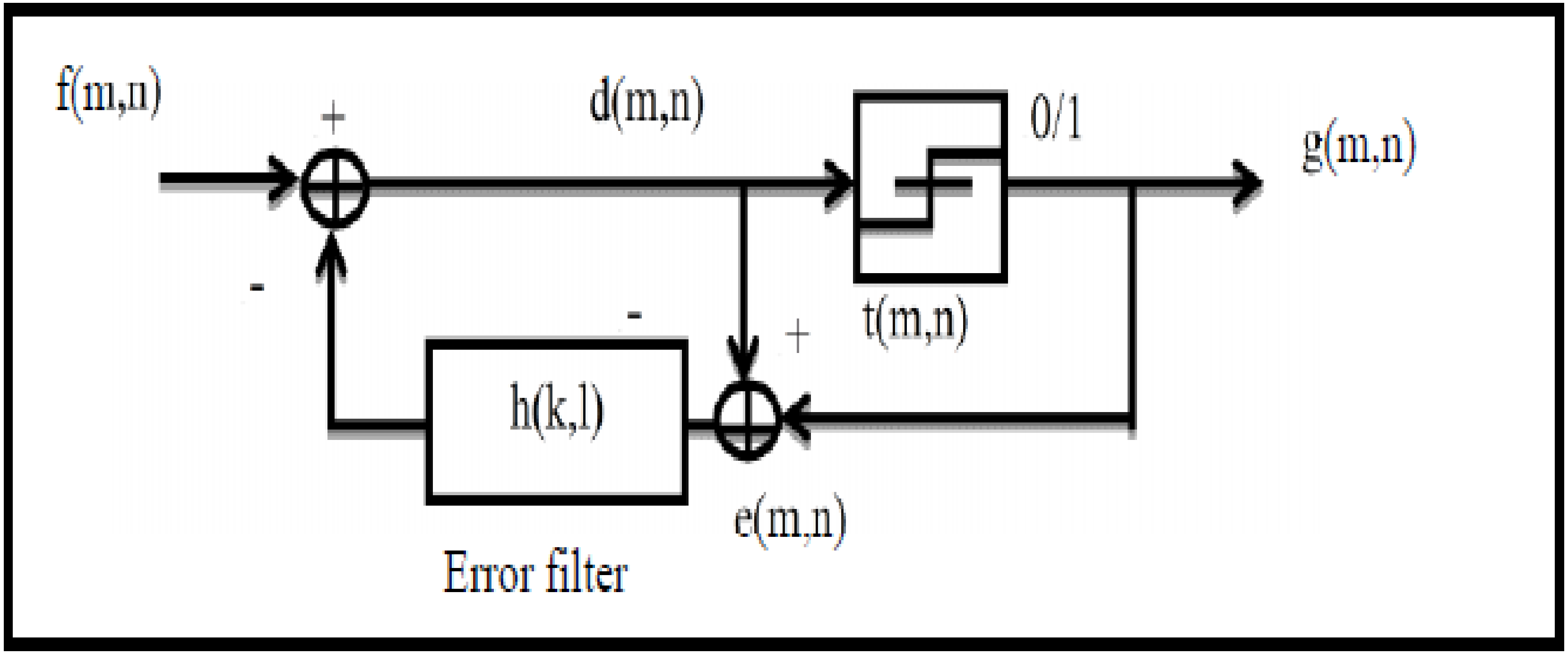
$\frac{1}{16} \times$

	●	7
3	5	1

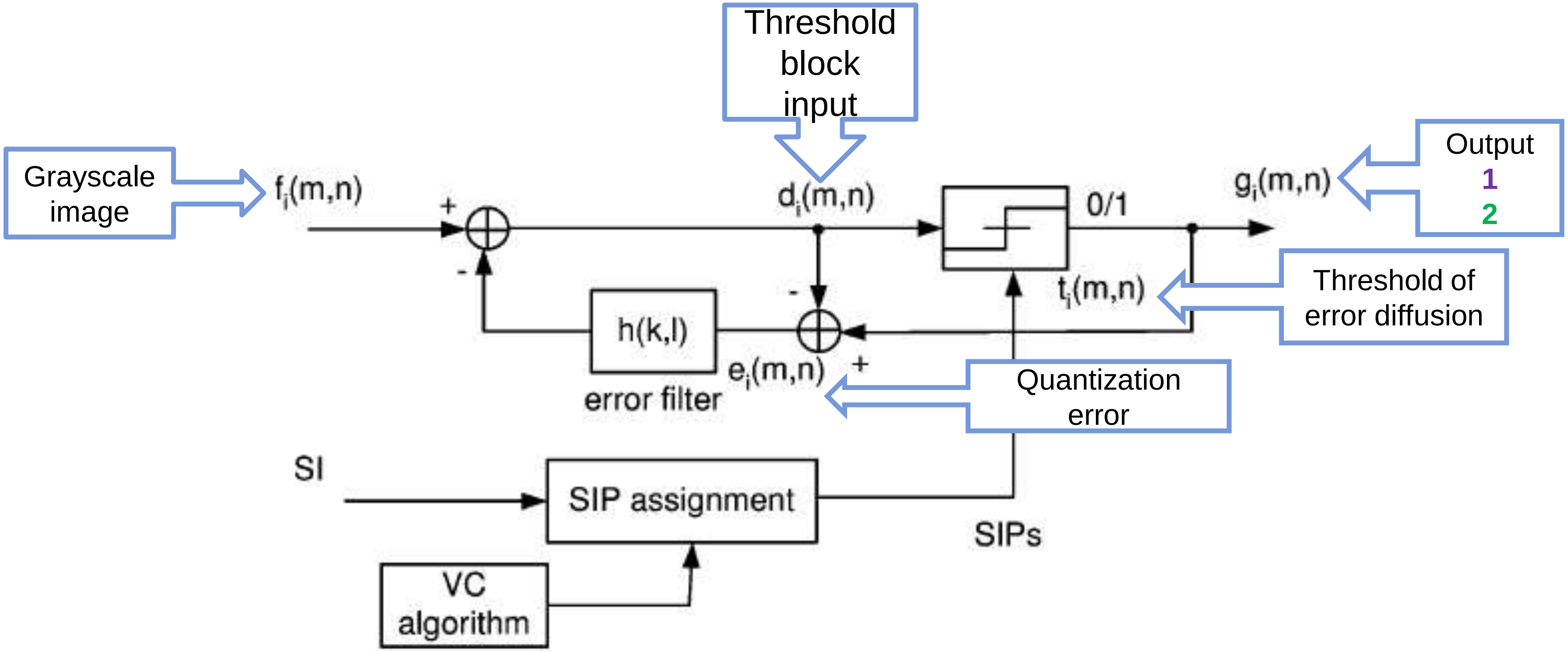
Floyd–Steinberg error filter. ● indicates the current pixel. The weights are given by: $h(0,1) = 7/16$, $h(1,-1) = 3/16$, $h(1,0) = 5/16$, and $h(1,1) = 1/16$.



Error diffusion



HVC via Error Diffusion



Block diagram of HVC using method 1. Depending on the secret image and VC scheme chosen, the SIP assignment block outputs the SIPs. If $g_i(m, n)$ is an SIP, its value is prefixed. Otherwise, $g_i(m, n)$ is determined by the output of the thresholding block.

THANK YOU