INVISIBLE COMMUNICATION FOR SECURITY AND AUTHENTICATION

Dr. Jyotsna Kumar Mandal

Professor of Department of Computer Science & Engineering,
Former Dean, ETM, Director, IQAC, University of Kalyani

Kalyani, Nadia, West Bengal

E-mail:jkmandal@klyuniv.ac.in, jkm.cse@gmail.com

Mobile:91 9434352214

OBJECTIVE

- Problem in Communication
- Steganography
- Work Related Objective

jkm.cse@gmail.com

COMMUNICATION

Security aspects

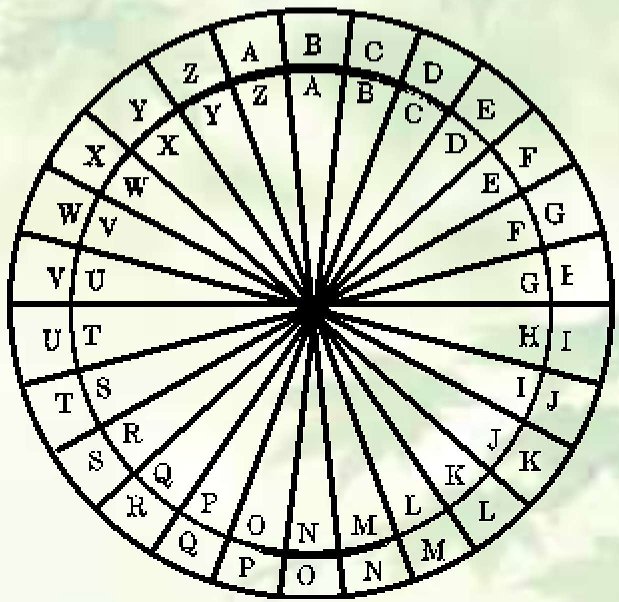
CRYPTOGRAPHY

STEGANOGRAPHY

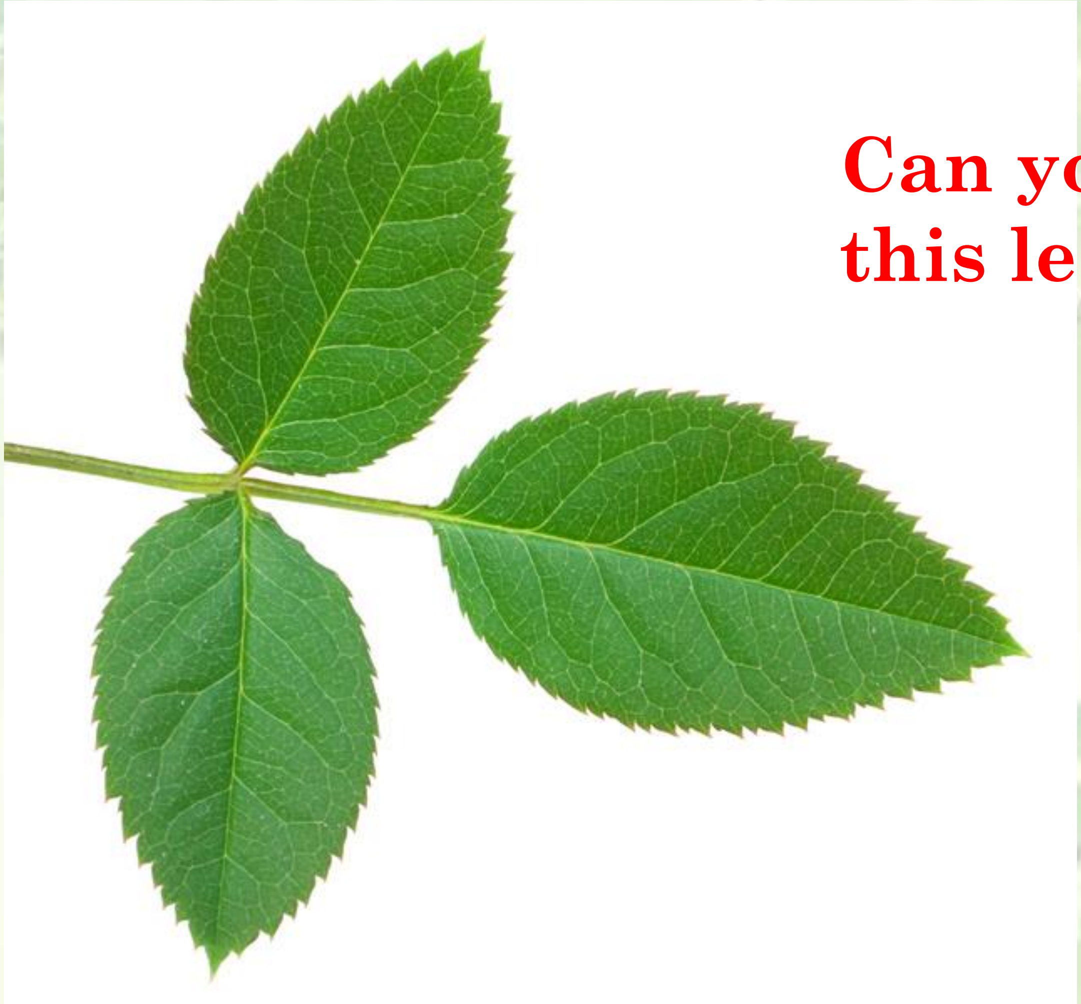
jkm.cse@gmail.com

CRYPTOGRAPHY

Plain Text



APPLICATION



Can you identify this leaf ?

Yes

jkm.cse@gmail.com

APPLICATION …. (CONT…)

Now Can you identify this leaf ?

May be Yes

jkm.cse@gmail.com

APPLICATION …. (CONT…)

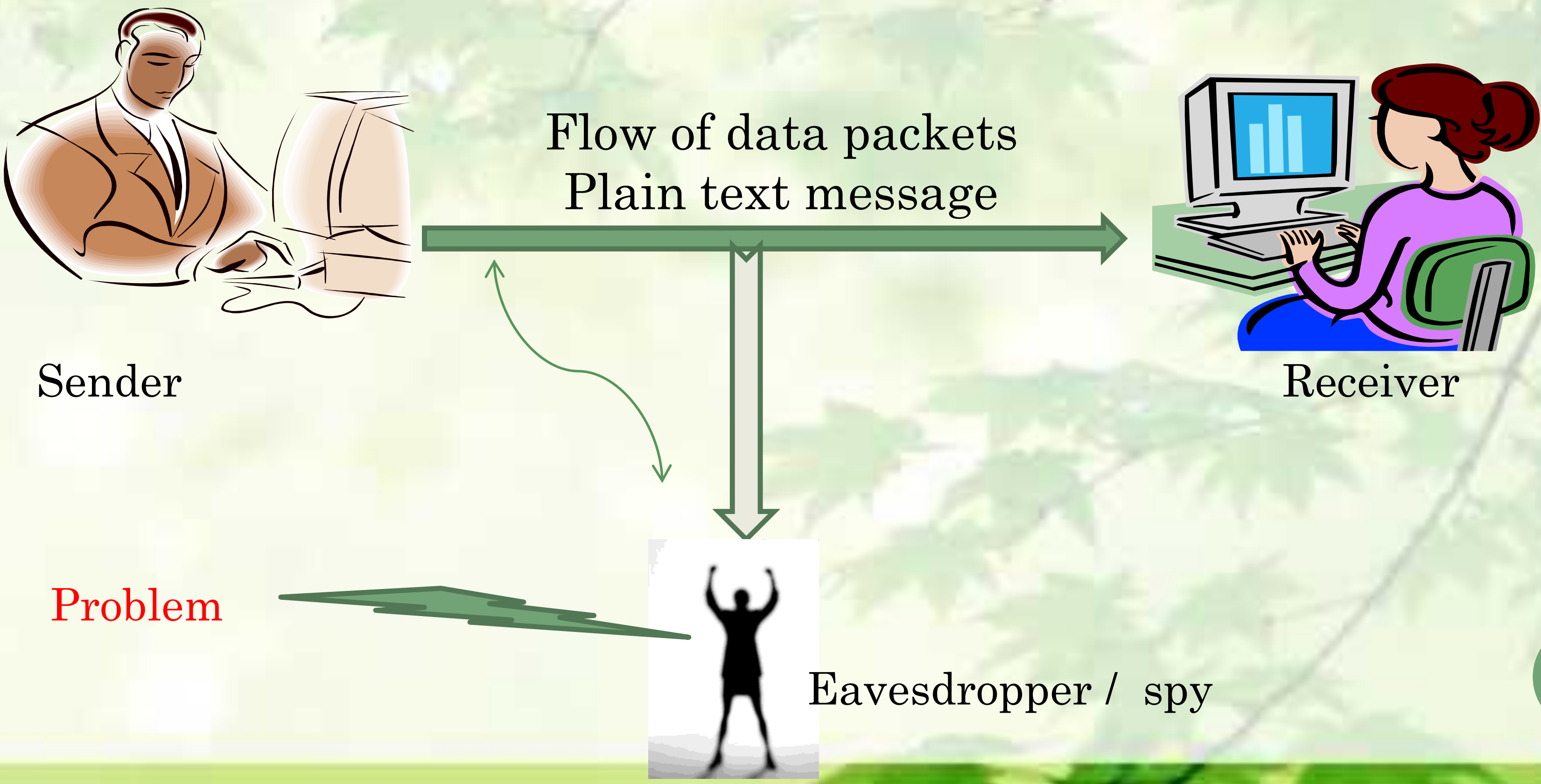
Now Can you?

No

Technology says YES through embedded information in the image.

jkm.cse@gmail.com

COMMUNICATION THROUGH NETWORK

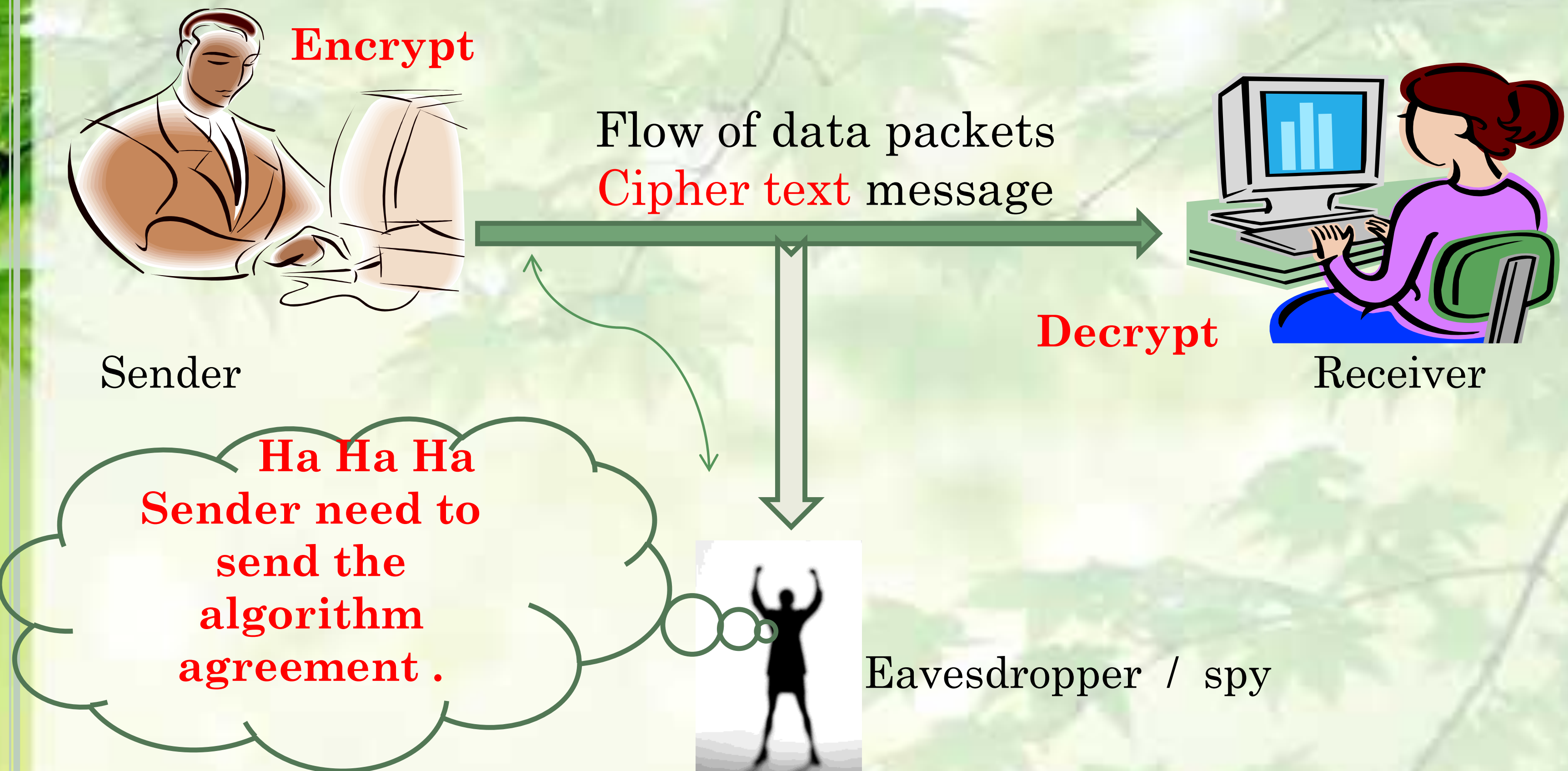


Plain text to Cipher text

- Substitution Techniques
  - Caesar Cipher
  - Mono-alphabetic Cipher
  - Homophonic Substitution Cipher
  - Playfair Cipher…………….
- Transposition Techniques
  - Rail Fence Technique
  - Vernam Cipher(One Time Pad)
  - Book Cipher/ Running key cipher………….

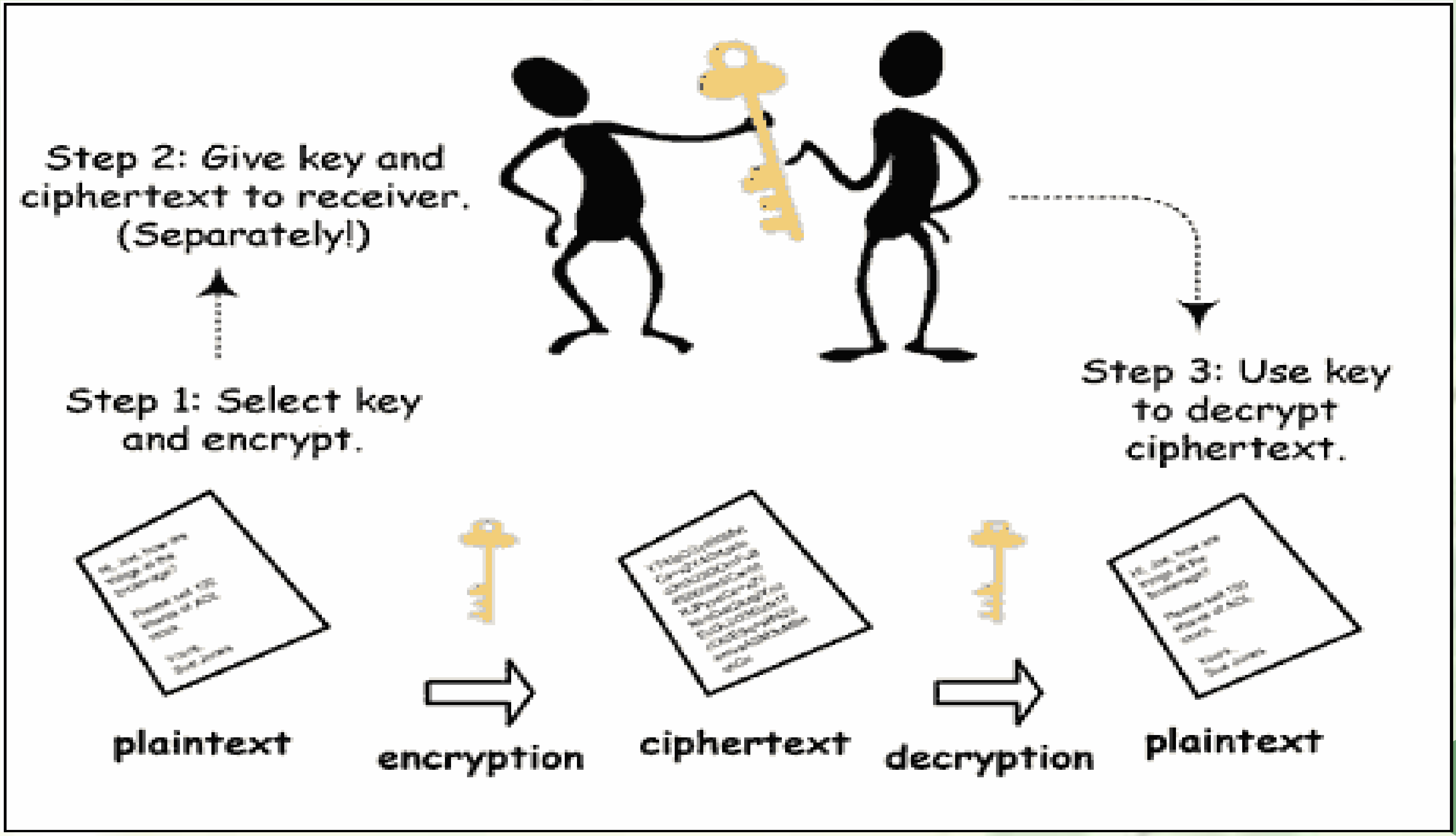
Encryption Decryption Technique...

Communication…….

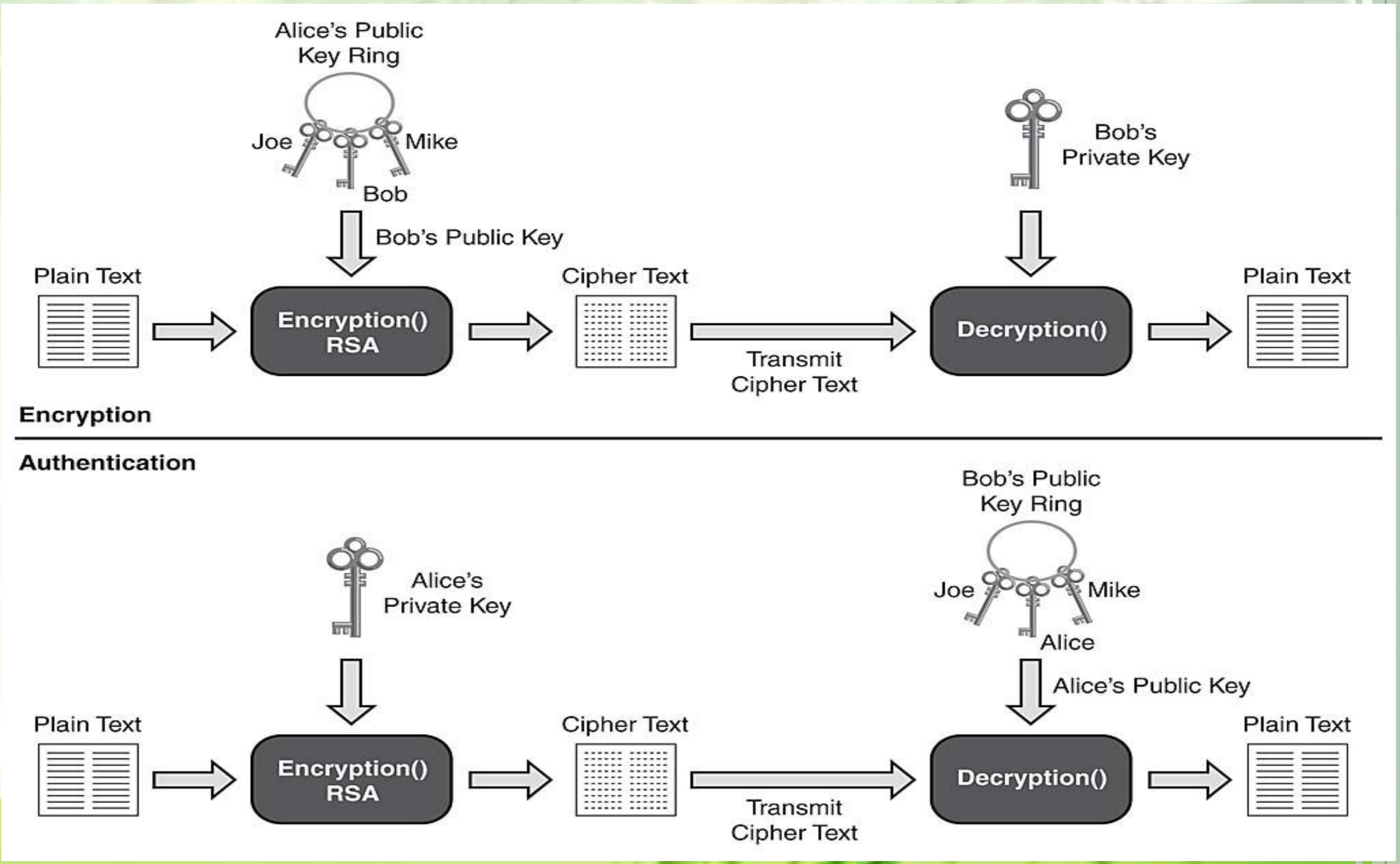


Note:- The decryption algorithm must be the same as the encryption algorithm. Otherwise decryption would not be able to retrieve the original message.

APPLICATIONS OF SYMMETRIC ALGORITHMS



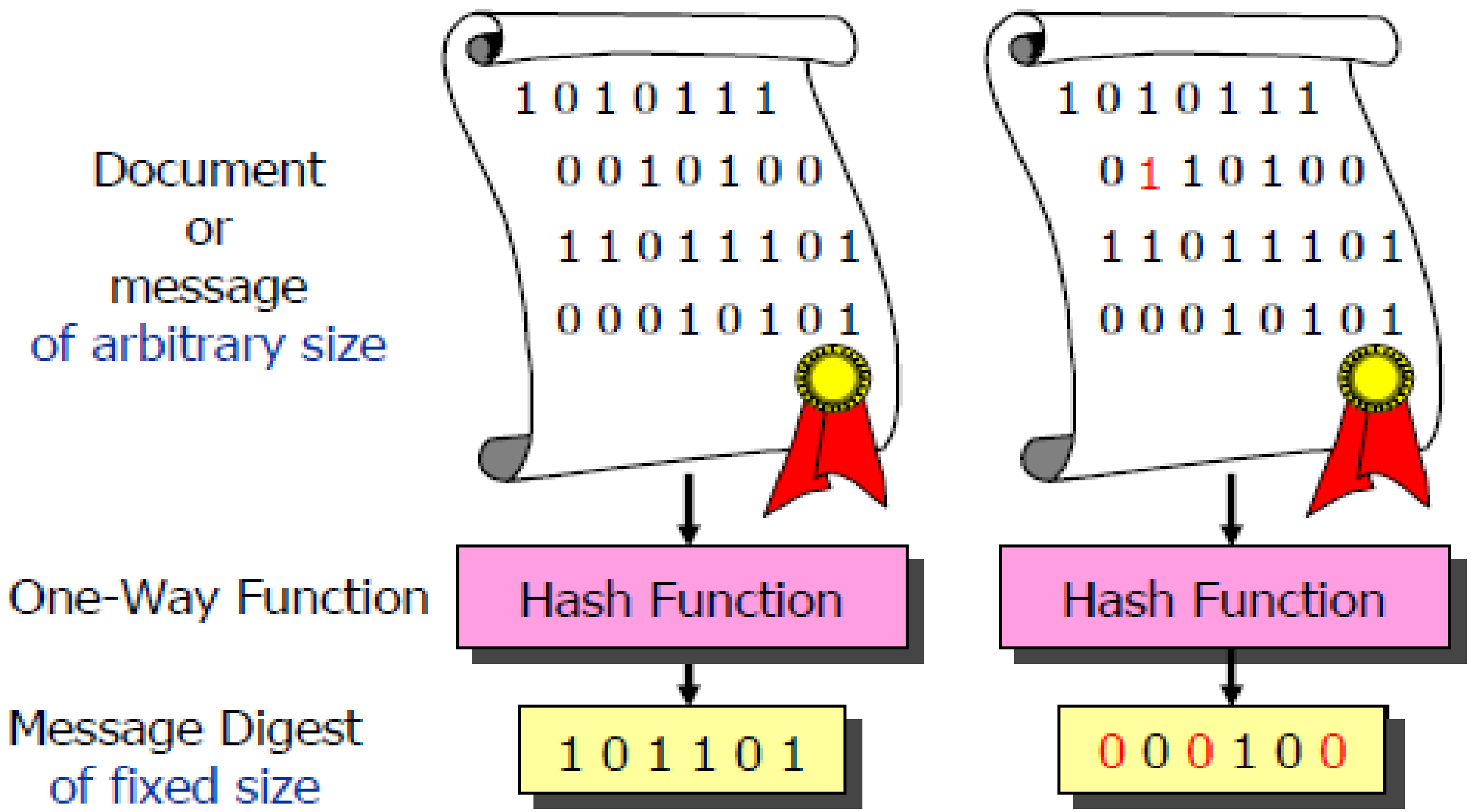
Applications of Asymmetric Algorithms



DIGITAL SIGNATURES

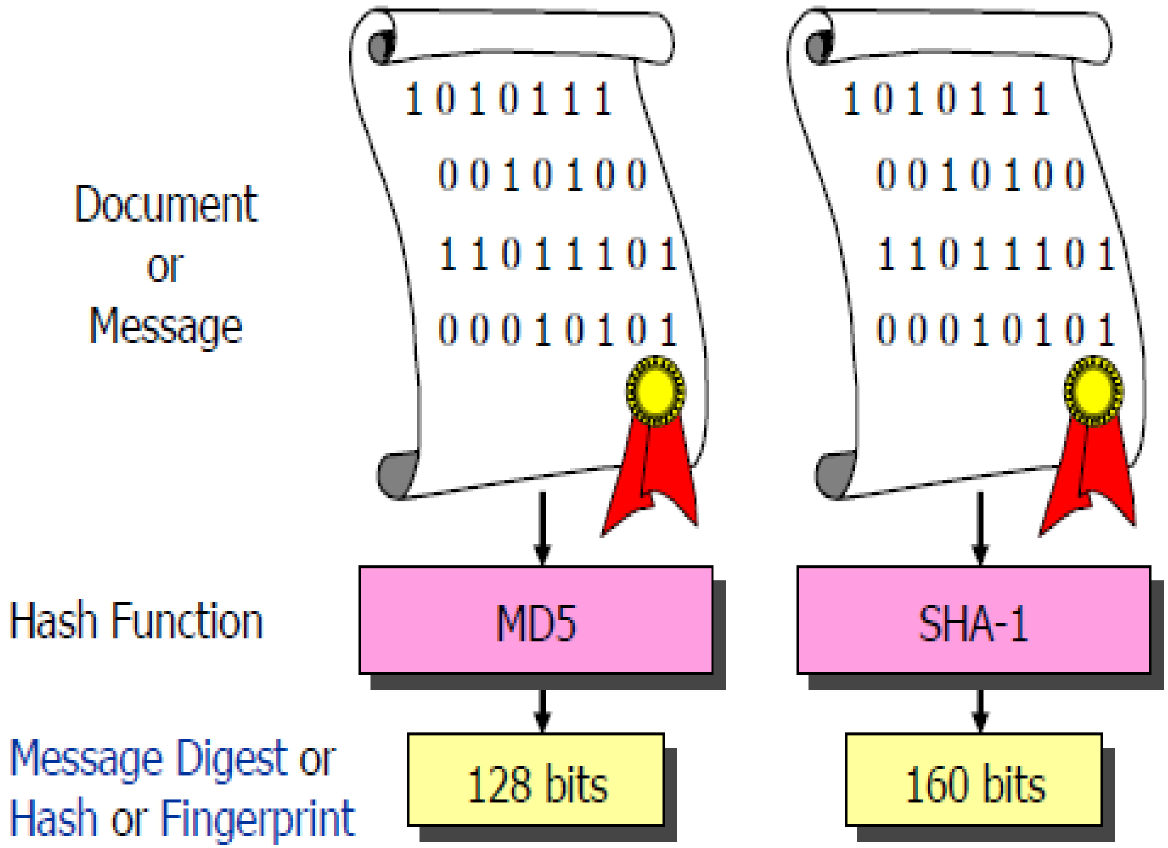
- A signature is a technique for non-repudiation based on the public key cryptography.
- The creator of a message can attach a code, the signature, which guarantees the source and integrity of the message.

MESSAGE DIGESTS :ONE–WAY HASH FUNCTIONS



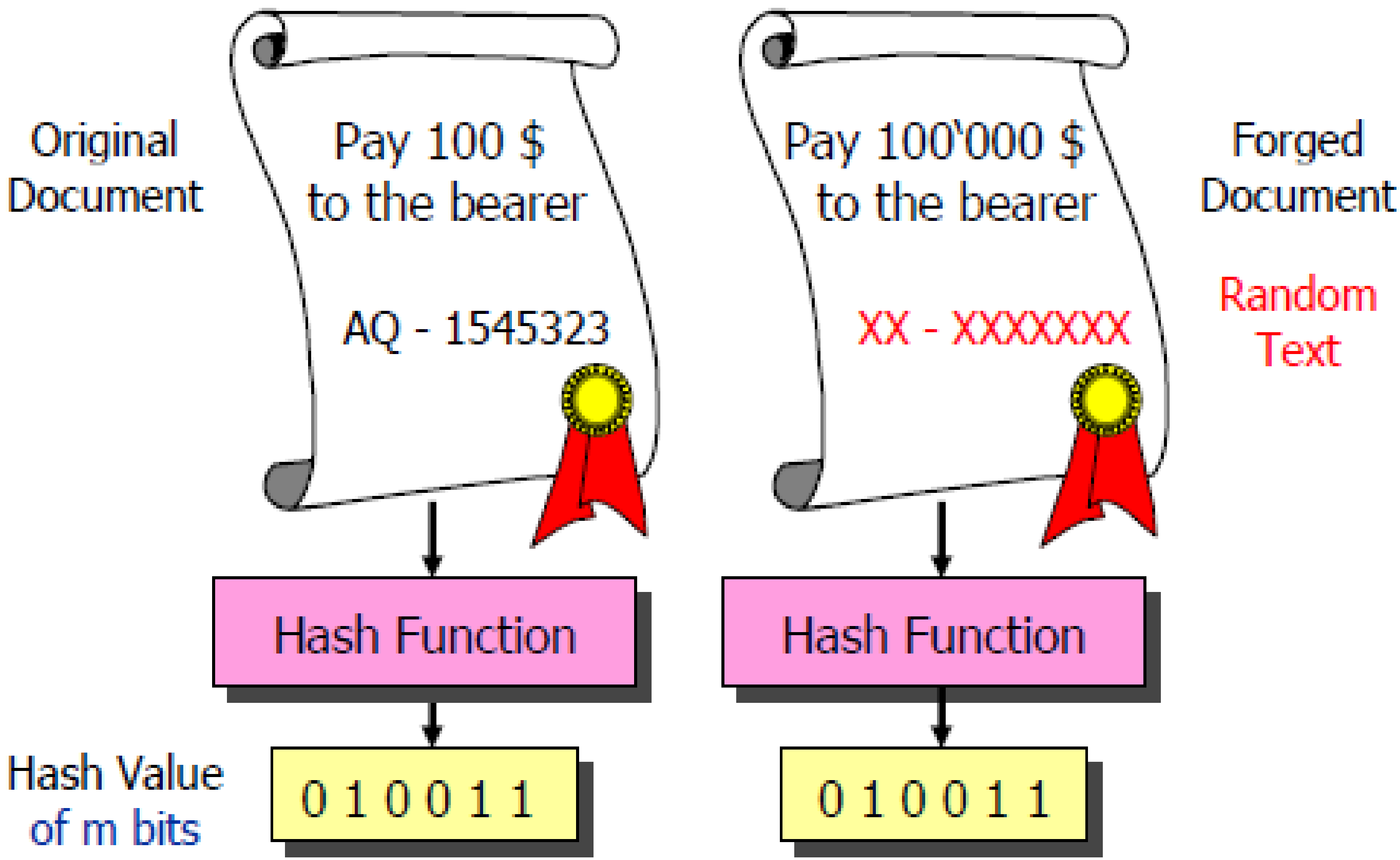
- A single bit change in a document should cause about 50% of the bits in the digest to change their values !

Popular Hash Functions



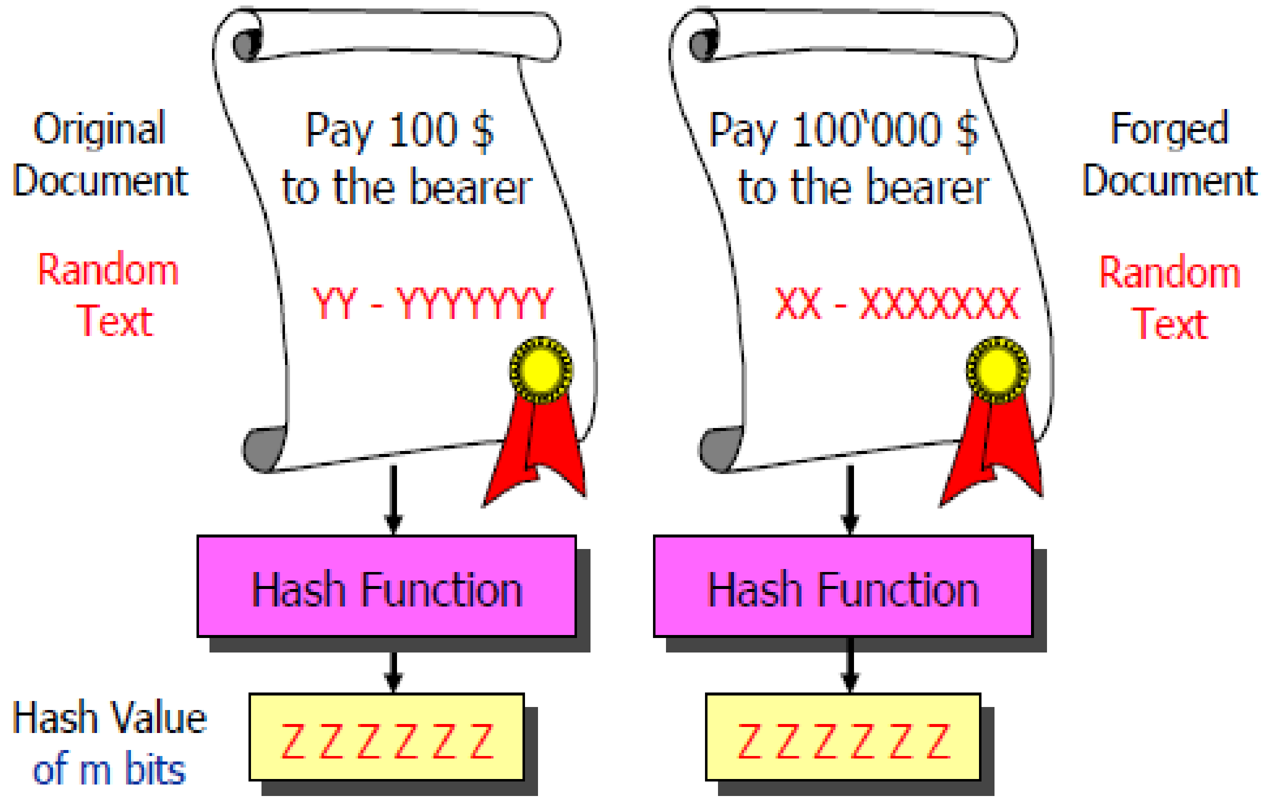
- MD5 – Message Digest # 5, Ron Rivest, RSA
- SHA-1 – Secure Hash Algorithm, NIST / NSA

Forging Documents



- On average 2^m trials are required to find a document having the same hash value as a given one !

Birthday Attacks against Hash Functions Looking for Collisions !



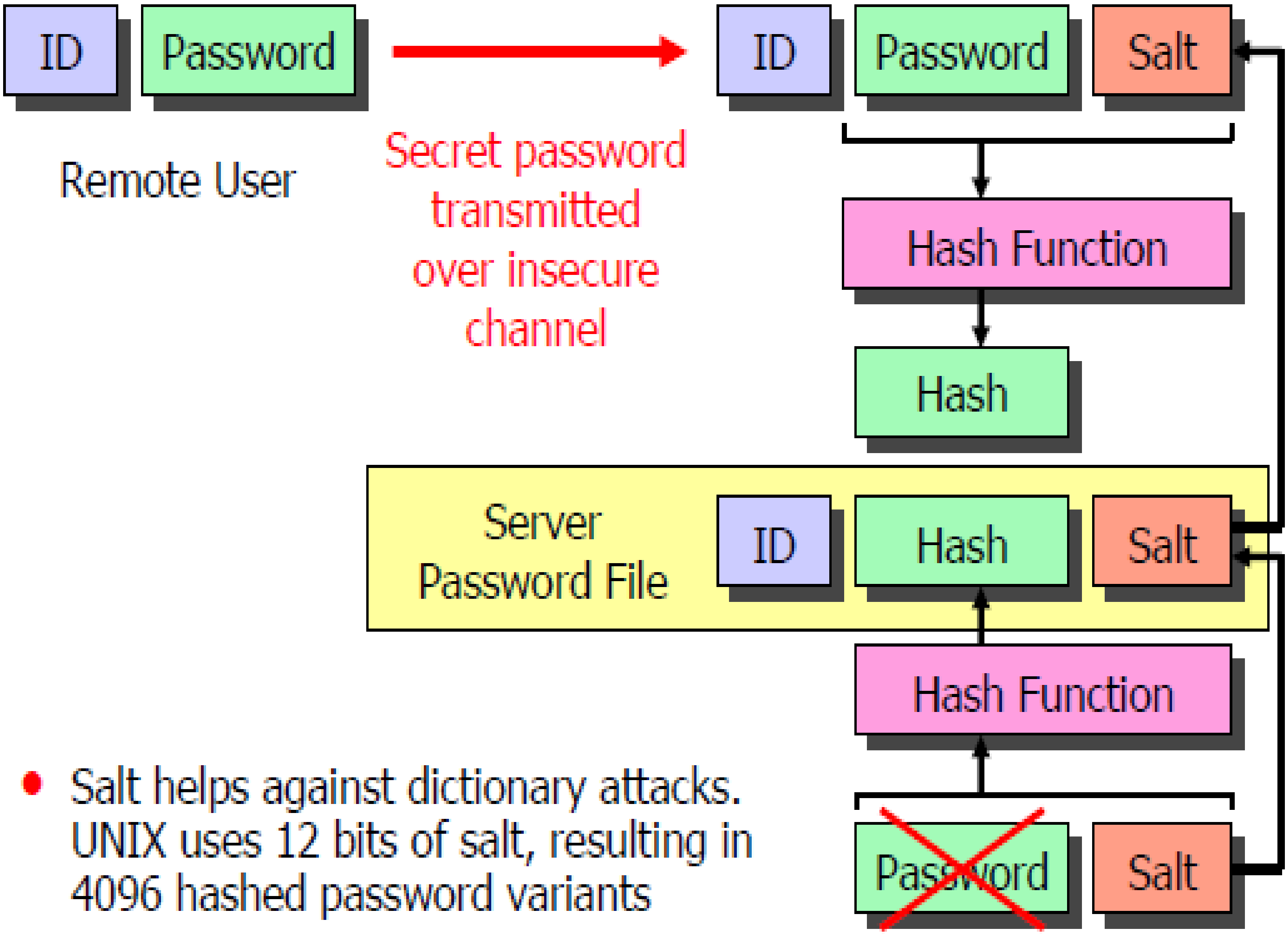
- Less than $2^{m/2}$ trials are required to find two documents having the same hash value $\Rightarrow$ MD5 with 2^{39} and SHA-1 with 2^{63} trials are both insecure !

User Authentication

"On the Internet, nobody knows you're a dog."

- Username / Password
  Dictionary Attacks
- One-Time Passwords
  Token: SecureID, etc.
- Public Key Algorithms
  Smartcards, Certificates, Public Key Infrastructure
- Biometrical Methods
  Fingerprint, Iris-Scan, Voice, Face, Hand, etc.

Insecure Authentication based on Passwords



- Salt helps against dictionary attacks. UNIX uses 12 bits of salt, resulting in 4096 hashed password variants

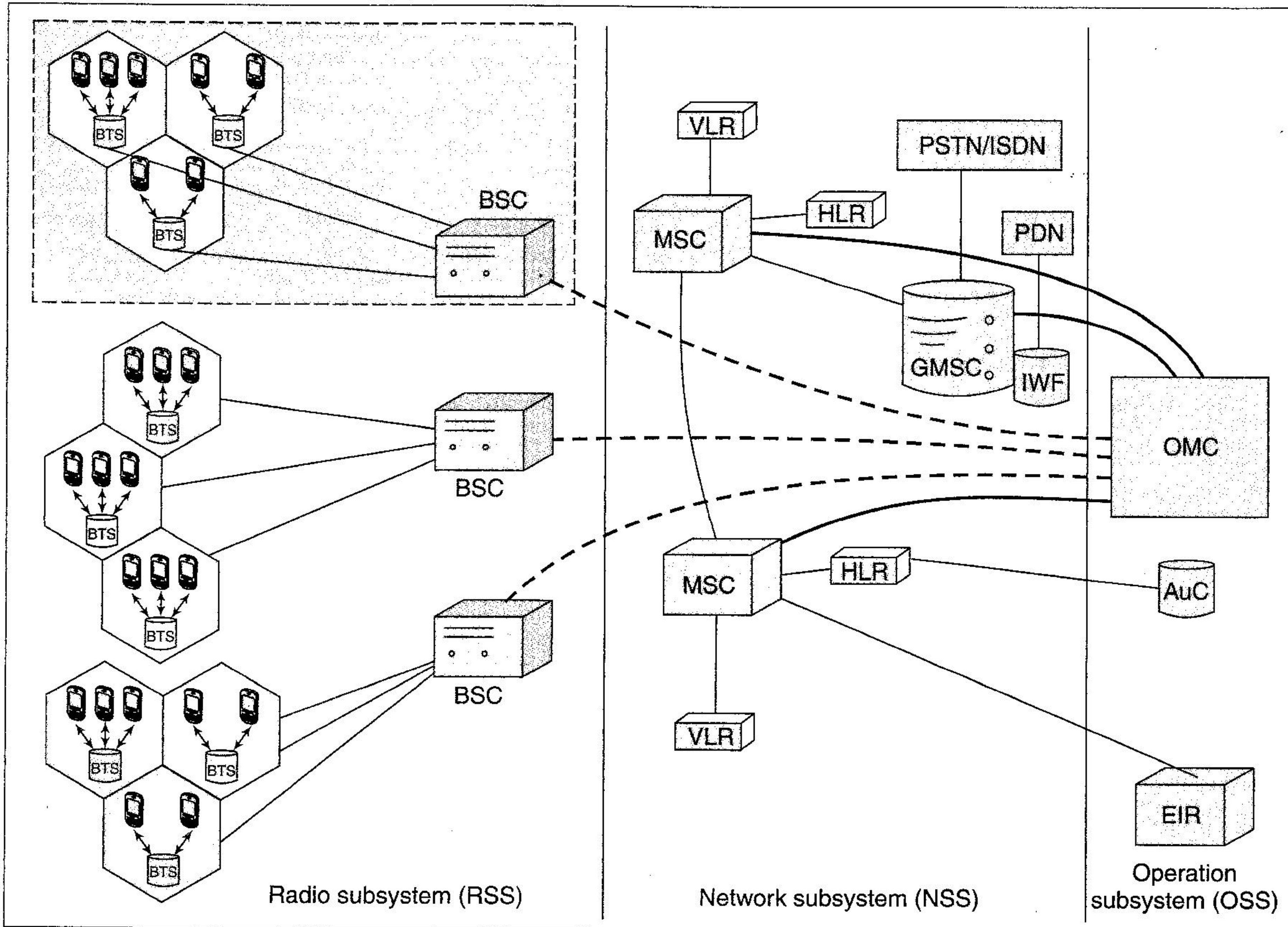


Fig. 3.2 GSM network architecture

EAVESDROP / SPY

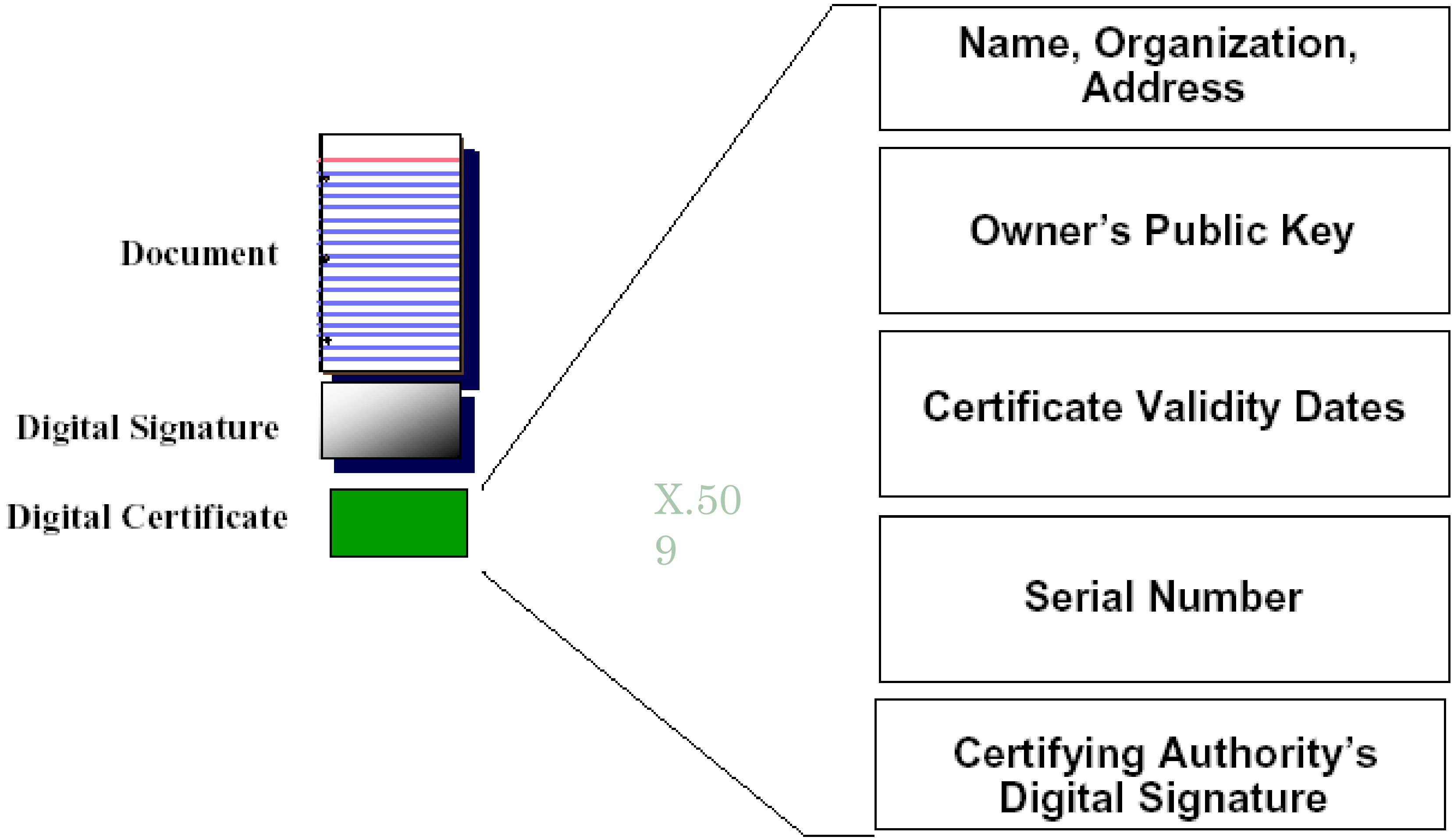
The Main intention of Eavesdrop is to change the information in mid of the way, but the receiver cant able to understand that.

For this

The Concept of **Digital Certificates** can be used.

Jkm.cse@gmail.com

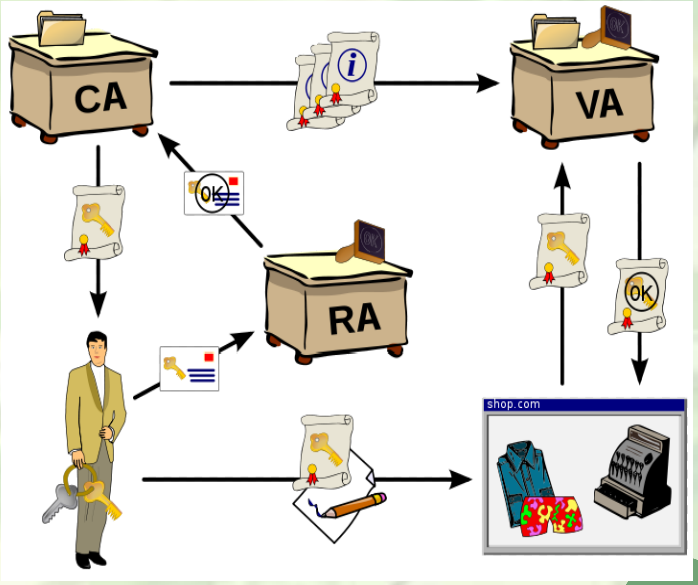
DIGITAL CERTIFICATES



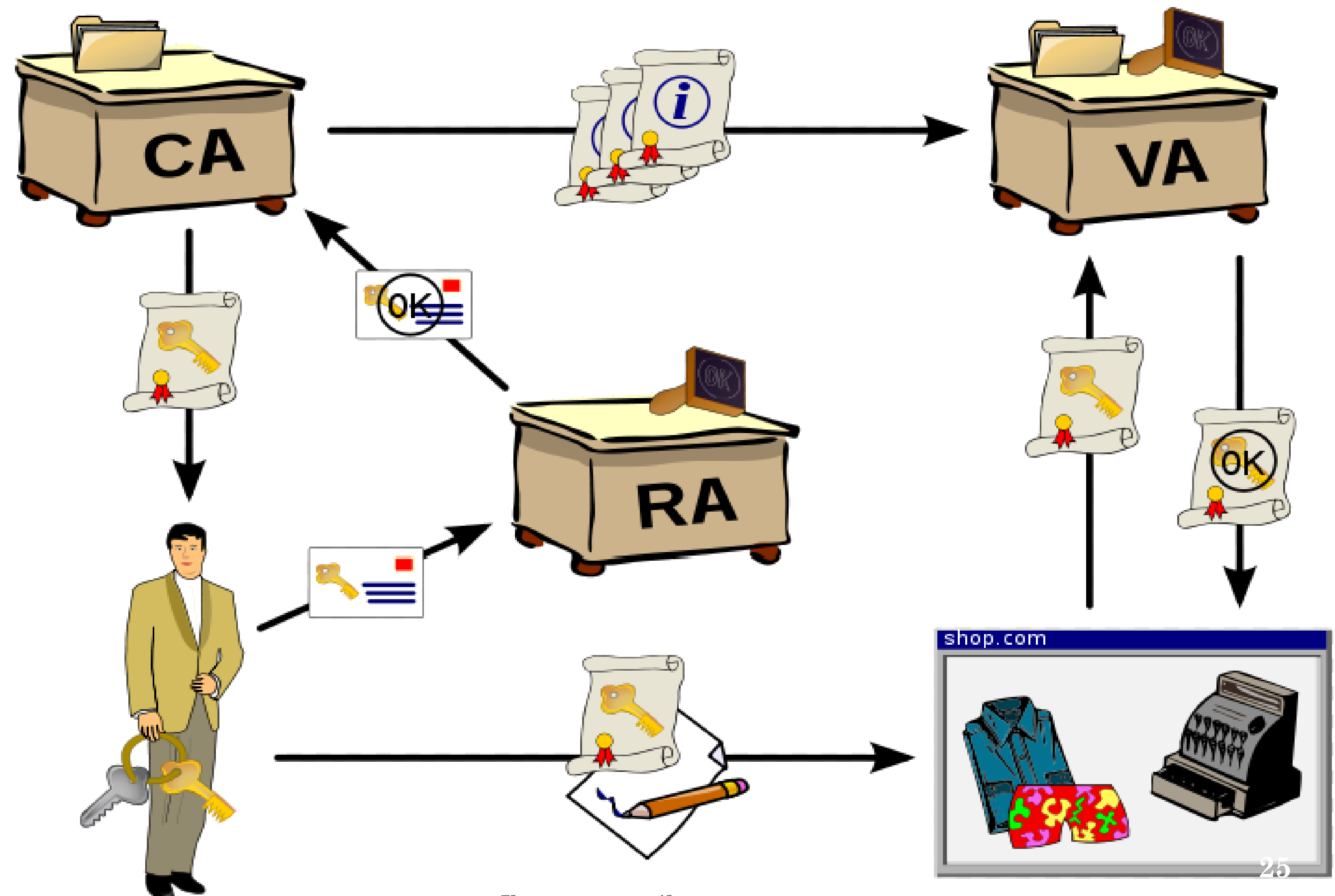
PUBLIC KEY INFRASTRUCTURE

The **Public Key Infrastructure** (**PKI**) is the road ahead for almost all cryptography system.

The **PKI** is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates .



PUBLIC KEY INFRASTRUCTURE



Jkm.cse@gmail.com

PROBLEM DOMAIN

- Data Security
  - Cryptography
  - Water Marking
  - Steganography
    - Image and Legal Document Authentication

- Steganography
  - In Spatial Domain
  - In Frequency Domain
    - Image Authentication by
    - Image Authentication by Message

STEGANOGRAPHY

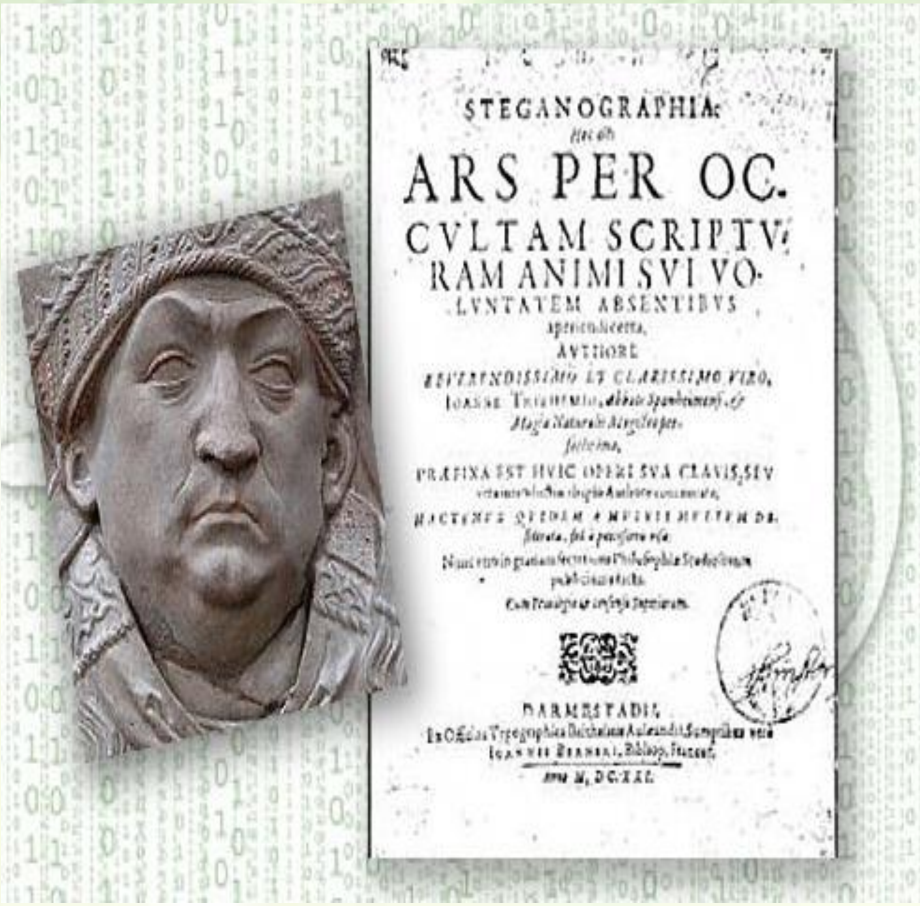
Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity (darkness).

- ✓Data Hiding
- ✓Secret message transmission
- ✓Ownership verification
- ✓Copyright Protection

jkm.cse@gmail.com

SECRET COMMUNICATION

Brief history of how the art and science has evolved.



The word steganography came from a 15th century work called Steganographia by a German abbot named Trithemius. On the face of it, the three books were about magic, but they were also contained an encrypted treatise on cryptography – so Steganographia was itself a case of steganography.

Second Example

An ancient Greek named Histaiaeus was fomenting revolt against the king of Persia and needed to pass along a message secretly. He shaved the head of a slave, tattooed the message on his scalp, then sent him on his way when his hair grew back in. Recipients of the message shaved his head again to read the alert. The Greeks used the same trick shaving and writing on the belly of a rabbit.

Third Example

Sometime in the 5th century B.C., an exiled Greek named Demaratus wrote a warning that the Persians planned to attack Sparta. He wrote the message on the wooden backing for a wax tablet, then hid it by filling in the wood frame with wax so it looked like a tablet containing no writing at all. The wife of the Spartan king divined that there was a message behind the wax, so they scraped it off and got the warning in time to set up a desperate defence at Thermopylae, incidentally giving modern screenwriters the plot for the movie The 300.

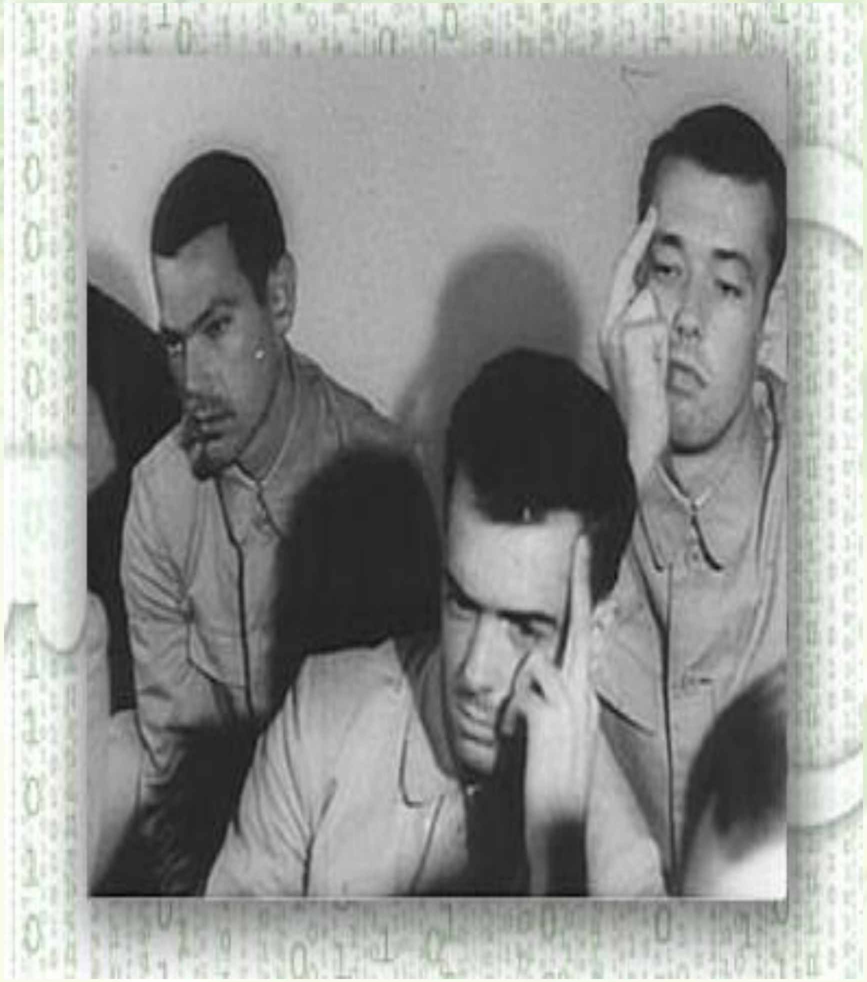
FOURTH EXAMPLE

Encoded messages have been knitted into sweaters and other garments. In this example, the blue dotted lines are Morse Code for, "My girlfriennd knit this." Yes, the sweater has a typo – an extra n in girlfriend - according to the woman who knitted it.

FIFTH EXAMPLE

During World War II, microdots - miniaturized photos that can be hidden in plain sight, then read using magnifiers – were used by spies to carry data out of enemy countries. Here the microdot circled in red piggybacks on a watch face. Blown up, it reveals a message written in German.

SIXTH EXAMPLE



When the USA Pueblo was captured by North Korea in 1968, the crew was forced to pose for propaganda photos to demonstrate they were being well treated. Their finger gestures are a form of steganography that sends a message Americans could decrypt right away, the North Koreans, not so quickly.

SEVENTH EXAMPLE

Digital photo steganography uses code fields for unimportant bits as places to hide encoded messages or images. While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. In these pictures, the image of the cat has been embedded in the image of the branches against the sky.

OWNERSHIP PROTECTION & VERIFICATION

Problem is Quality of Stego Image

Secret Code

Sender Side

km.cse@gmail.com

INSERTION TECHNIQUE

65	78	73	30
58	78	38	32
56	73	56	35
59	70	52	39

Original Image
(Image Matrix)

01000001	01001110	01001001	00011110
00111010	01001110	00100110	00100000
00111000	01001001	00111000	00100011
00111011	01000110	00110100	00100111

10011001	11100101	10011101	11001101

Secret Data

01000001	01001100	01000101	00010111
00111011	01001010	00101010	00100001
00111001	01001101	00111100	00100011
00111011	01000000	00111100	00100111

jkm.cse@gmail.com

Insertion Technique

010000**01**	01001**10**0	0100**01**01	0001**0**11**1**
001110**11**	01001**01**0	00101**01**0	0010**0**00**1**
001110**01**	01001**10**1	00111**1**00	0010**0**01**1**
001110**11**	01000**00**0	00111**1**00	0010**0**11**1**

65	76	69	23
59	74	42	33
57	77	60	35
59	64	60	39

Image with Secret Data

65	78	73	30
58	78	38	32
56	73	56	35
59	70	52	39

Original Image

jkm.cse@gmail.com

STEGANOGRAPHY

- TRADITIONAL STEGANOGRAPHY.

- MODERN STEGANOGRAPHY.

Steganographic Protocols

- ❖ Pure Steganography
- ❖ Secret Key Steganography
- ❖ Public Key Steganography

Applications Steganography

1. Usage in modern printers

   Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2. Usage in Legal document

   Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified, copyright protection, Bank draft, cheque and many other.

3. Steganography in audio can be used with mobile phone.

Rumored Usage in Terrorism

Rumors about terrorists using steganography started first in the daily newspaper USA Today on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July of the same year, the information looked even more precise: "Militants wire Web with links to jihad".

Document Authentication

Technique to Authenticate

Document Authentication

We are Indian. We are proud for our country. We always like to look ahead with positive attitude and giving maximum effort to growth our country. We are so much strong in science and Technology.

Nabin Ghoshal

We are Indian. We are proud for our country. We always like to look ahead with **negative attitude** and giving **minimum effort** to growth our country. We are so **much weak in** science and Technology.

Nabin Ghoshal

Document Authentication

Extract MD5

Compare

Generate MD5

We are Indian. We are proud for our country. We always like to look ahead with negative attitude and giving minimum effort to growth our country. We are so much weak in science and Technology.

Nabin Ghoshal

Image Authentication

Lena Image

Lena Image

SENDER SIDE OPERATION

Image Authentication

Embedded Lena Image

Original Secret Image

COMPARE

Extracted Image

RECEIVER SIDE OPERATION

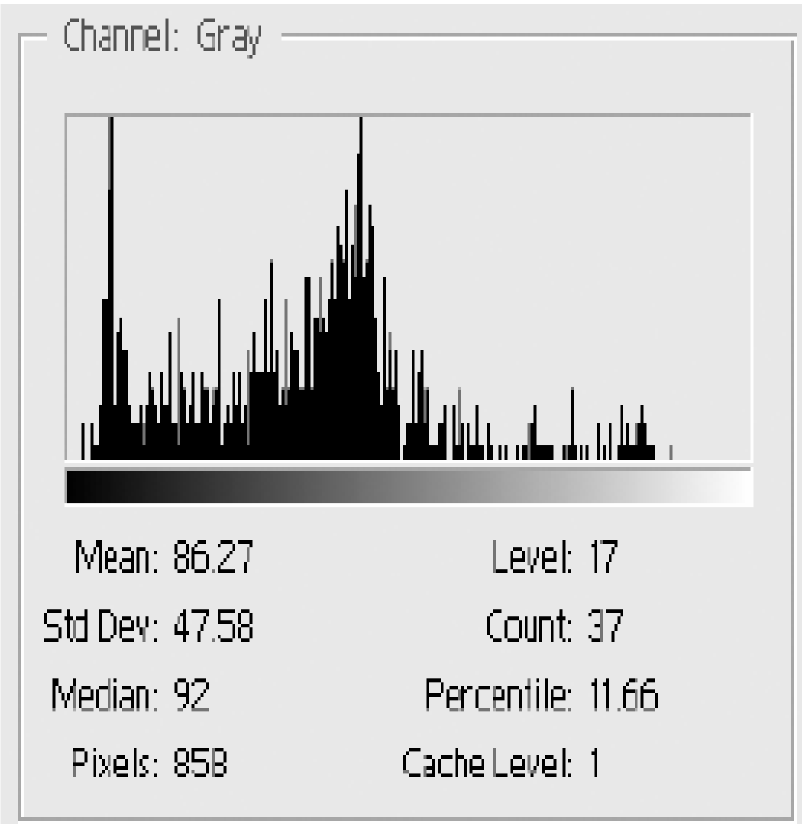
Authentication and Secret Message Transmission Technique Using Discrete Fourier Transformation.

(a). Hill. (b). Lotus. (c). ASMTDFT. (d). S-tools.

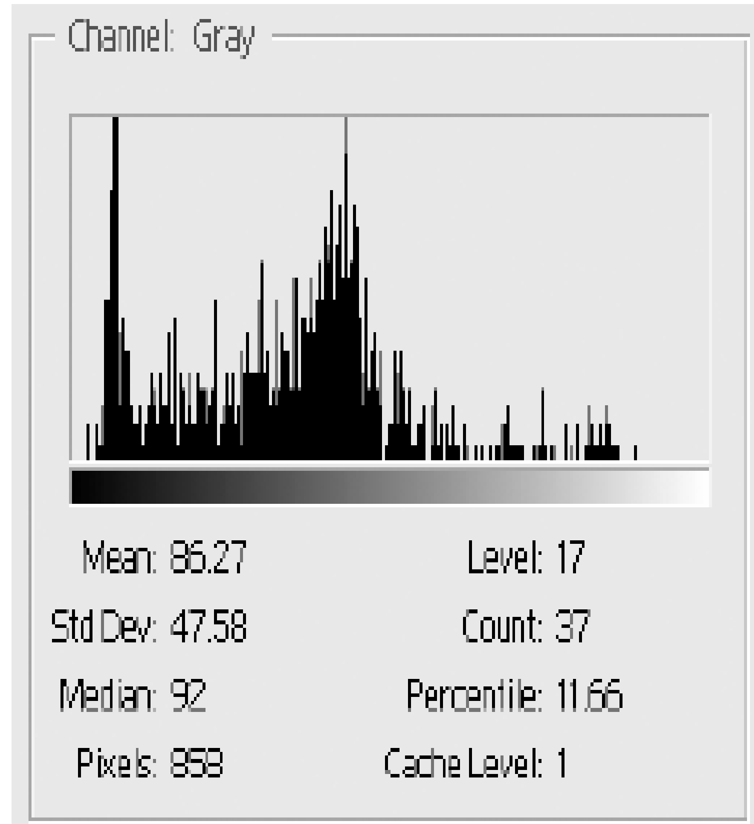
Figure 3. Comparison of visual fidelity in embedding 'Lotus' using ASMTDFT and S-Tools.

(a). Rashmancha. (b). Lotus. (c). ASMTDFT. (d). S-tools.

Figure 4. Comparison of visual fidelity in embedding 'Lotus' using ASMTDFT and S-Tools.



(a). Lotus.



(b). Extracted Lotus.

. Histogram for authenticating image 'Lotus', extracted image 'Lotus' using ASMTDFT.

Objectives of Image Steganography

Data Hiding

Secured message Transmission

Invisible data transmission

Ownership verification

Embedding/ Authentication

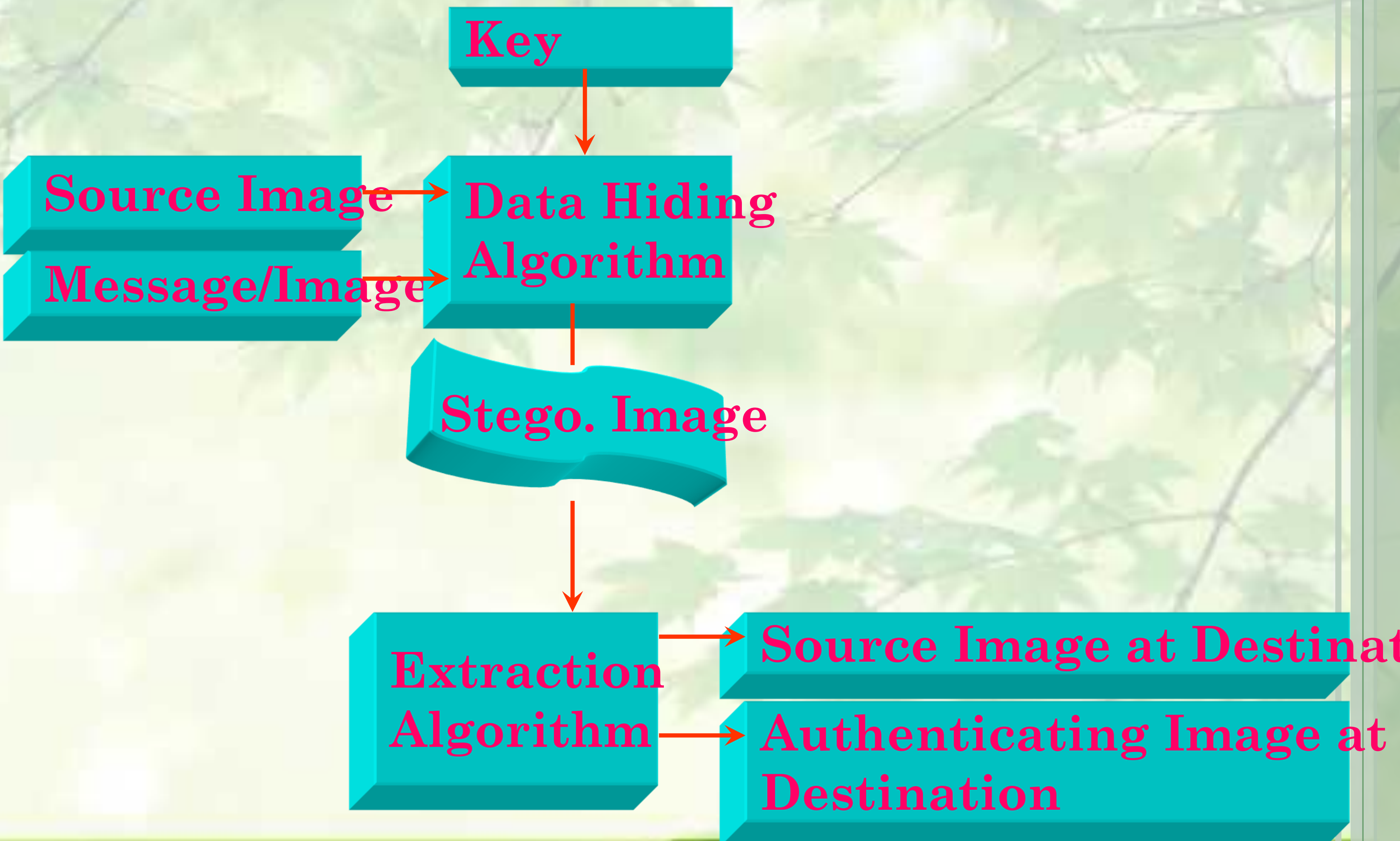


IMAGE STEGANOGRAPHY

Source Image Lenna

Authenticating Image Earth

Authenticated Image Lenna

IMAGE STEGANOGRAPHY

Source Image Peppers

Authenticating Image

Embedded Image Peppers

TECHNICAL ASPECTS

SPATIAL DOMAIN LSB

STEGONAGRAPHY

LSB (Least Significant Bit)

149	13	201
150	15	202
159	16	203

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

HIDE --- 365

1 0 1 1 0 1 1 0 1

HIDE --- 365

1 0 1 1 0 1 1 0 1

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Changed data

1001010**1**	0000110**0**	1100100**1**
1001011**1**	0000111**0**	1100101**1**
1001111**1**	0001000**0**	1100101**1**

Thus, we have successfully hidden 9 bits in 9 bytes but at a cost of only changing 4bit, or roughly 50%, of the LSBs.

FREQUENCY DOMAIN STEGONAGRAPHY

- **DISCRETE FOURIER TRANSFORMED**
- **DISCRETE COSINE TRANSFORMED**
- **DISCRETE WAVELET TRANSFORMED**
- **Z-TRANSFORMED**

MIXED DOMAIN STEGONAGRAPHY

- **SPATIAL DOMAIN**
- **FREQUENCY DOMAIN**

BOTH DOMAINS ARE USED IN THIS STEGONAGRAPIC PROCESS

TRANSFORMED TECHNIQUED

SPECIFICATIONS

- Embedding is done in frequency components
- Source image 512 x 512
- Authenticating image 128 x 128
- Embedding done on Real components

IMAGE STEGANOGRAPHY

Source Image Peppers

Source Image Lenna

FREQUENCY DOMAIN STEGONAGRAPHY

- **DISCRETE FOURIER TRANSFORMED**
- **DISCRETE COSINE TRANSFORMED**
- **DISCRETE WAVELET TRANSFORMED**
- **Z-TRANSFORMED**

DFT and IDFT

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\, e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

where u = 0 to M – 1 and v = 0 to N-1.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v)\, e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

where x = 0 to M – 1 and y = 0 to N-1.

$F(u, v) = \frac{1}{2}\sum\sum f(x, y)[\cos 2\Pi(ux / 2 + vy / 2) - i \sin 2\Pi(ux / 2 + vy / 2)] = \sum\sum f(x , y) [\cos \Pi (ux + vy) - i \sin \Pi(ux + vy)]$

where x, y are spatial variables and u, v are frequency variables

Formulation and Motivation of DFTMCIAWC

2 x 2 mask values are {a, b, c, d} from the source image. The DFT values are $F(a) = ½ (a + b + c + d) = W$ (say), $F(b) = ½ (a – b + c – d) = X$ (say), $F(c) = ½ (a + b – c – d) = Y$ (say), and $F(d) = ½ (a – b – c + d) = Z$ (say) for four a, b, c, and d spatial values and W, X, Y and Z are frequency values respectively.

Formulation and Motivation of DFTMCIAWC

Spatial Domain to Frequency Domain (DFT)

$F(a) = \frac{1}{2}\,(a + b + c + d) = W$
$F(b) = \frac{1}{2}\,(a - b + c - d) = X$
$F(c) = \frac{1}{2}\,(a + b - c - d) = Y$
$F(d) = \frac{1}{2}\,(a - b - c + d) = Z$

DFT to Spatial Domain (IDFT)

$F^{-1}(W) = \frac{1}{2}\,(W + X + Y + Z)$
$F^{-1}(X) = \frac{1}{2}\,(W - X + Y - Z)$
$F^{-1}(Y) = \frac{1}{2}\,(W + X - Y - Z)$
$F^{-1}(Z) = \frac{1}{2}\,(W - X - Y + Z)$

Problems and Solutions of DFTMCIAWC

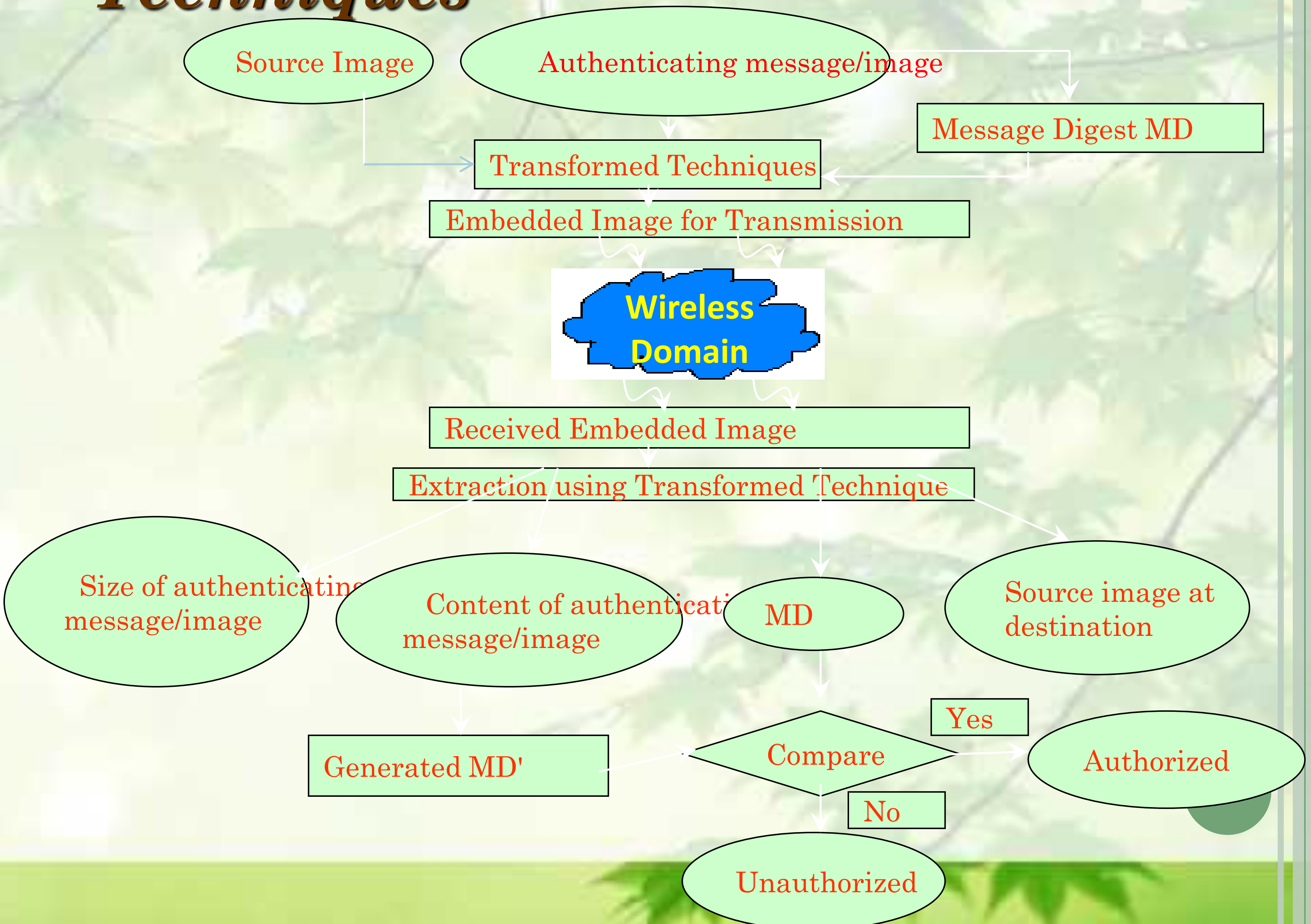
A. The converted value may by negative(-ve).

B. The converted value in spatial domain may be a fractional number.

C. The converted value may be greater the maximum value (i.e. 255).

Solutions: Re-adjustment is done on 1st frequency component where embedding is not done.

Flow Diagram of FD Techniques



Visual Interpretation

Source Image Lenna

Authenticating Image Earth

Authenticated Image Lenna

Results & Visual Interpretation using DFTMCIAWC

Source Image Peppers

Authenticating Image

Embedded Image using DFTMCIAWC

Correctness of Adjustment

The logic behind adding/subtracting 8 with two adjacent pixels:

If the range is shifted from lower to higher the embedded message become undetectable. To adjust pixels 8 is added or subtracted to bring the interval in the lower range. Again if you add or subtract 8 from P_i' or P_{i+1}' then 3-lsb bits in both cases will be unaltered as there will be change on 3rd bit position(from LSB(0th bit)) towards MSB.

P_i' after adjustment = 23 = 000 1 0 111

Unchanged Embedded bits

This bit has changed during handle

Correctness of Adjustment

- After embedding and before readjustment the pixel P_i' was 31_{10} = 0 0 0 1 1 1 1 1

  Adjustment -8_{10} =0 0 0 0 1 0 0 0

$P'_{i'}$ on readjustment = 0 0 0 1 0 1 1 1

Embedded information

This bit is changed in handling

After embedding and before readjustment the pixel P_{i+1}' was 8_{10} = 0 0 0 0 1 0 0 0

Adjustment $+8_{10}$ = 0 0 0 0 1 0 0 0

$P'_{i'+1}$ on readjustment = 0 0 0

No effect on information embedded

This bit changed in readjustment, no effect on information

New Difference after Adjustment

Calculate new range di = 23-16 = 7

The interval/range fabricated to lower range after adjustment

So there is no decoding error

Finally	Initially
Pi' =23	Pi =30
Pi+1'=16	Pi+1=15

Some Open Directions

- **Extension to more bits insertion within each Byte of pixel information in Color image.**
- **Extension to chose any dimension of Mask.**
- **Extension to change the direction of accessing of Image Mask (to column major order).**

ADJUSTMENT

10	25
30	20

ORIGINAL MATRIX REGENERATED THROUGH REVERSE TRANSFORM

TRANSFORM MATRIX

85	--20- 5J
-5	-20+5J

Let 85 is the median value of the block
Convert it to binary:

1010101

Embedding

85	--20- 5J
-5	-20+5J

Source Stream

85=1010101

Secrete Information 'S' is

1010011

Embed a bit into Fourth LSB

Embedded Stream:1011101

New Generation(GA Based Tuning)

85	--20-5J
-5	-20+5J

Source stream:1010101=85

One bit from Secrete Information 'S' (1010011) is 1 has been embedded into Fourth LSB

Embedded Stream:1011101

Pixel Value after embedding is:93

Difference:93-85=8

As next bit of embedded position is 1, flip all bits right to embedded bit to zero

Handled Embedded pixel:1011000=88

Original Pixel:85

Differenec:88-85 = 3 which is minimum

COVER IMAGE

10	25
30	20

TRANSFORMED COEFFICIENTS

85	--20- 5J
-5	-20+5J

EMBEDDED COEFFICIENTS

93	--20- 5J
-5	-20+5J

GA BASED ADJUSTMENT

88	--20- 5J
-5	-20+5J

GA BASED ADJUSTMENT

88	--20- 5J
-5	-20+5J

EMBEDDED EINVERSE TRANSFORMED

10	26
30	20

EMBEDDED EINVERSE TRANSFORMED

10	26
30	20

GA BASED CROSSOVER

12	25
24	18

Chaotic Maps for authentication

Recurrence Relation

$$X_{n+1} = \mu_2 X_n \text{ for } X_n < 1/2$$
$$\mu_2 X_n \text{ for } 1/2 <= X_n$$

$$Y_{n+1} = \mu_2 Y_n \text{ for } Y_n < 1/2$$
$$\mu_2 Y_n \text{ for } 1/2 <= Y_n$$

Random Bit Generator

$$G(X_{n+1}, Y_{n+1}) = 0 \text{ if } X_{n+1>=} Y_{n+1}$$
$$1 \text{ if } X_{n+1>=} Y_{n+1}$$

jkm.cse@gmail.com

SKEW TENT MAPS FOR AUTHENTICATION

$$X_{n+1} = P = X_i \ /\alpha \text{ for } X_i = [0, \alpha]$$
$$P' = 1 - X_i \ /(1-\alpha) \text{ for } X_i = [\alpha, 1]$$

Binary Bit Generator

$$\mathbf{G_{i+1} = 0 \text{ if } P < P' \text{ Else } 1}$$

jkm.cse@gmail.com

CROSS COUPLED MAP FOR AUTHENTICATION

$$X_{n+1} = X_i \ /\alpha \ \text{for} \ X_i = [0, \alpha]$$

$$Y_{n+1} = 1 - Y_i \ /(1-\alpha) \ \text{for} \ X_i = [\alpha, 1]$$

jkm.cse@gmail.com

Random Bit Generator

$$G(X_{n+1}, Y_{n+1}) = 0 \ \text{if} \ X_{n+1>=} Y_{n+1}$$

$$1 \ \text{if} \ X_{n+1>=} Y_{n+1}$$

Generation of chaotic map

- Equation of chaotic map:

$$X_{k+1} = \mu X_k(1 - X_k)$$

Here, $0 <= \mu <= 4$ and $0 < X_k < 1$

- the map is in chaotic region when

$$3.5699456 < \mu <= 4$$

- μ=control parameter, the sequence is non periodic and non convergent.

STEGANOGRAPHIC USE

- here, μ=3.60, X_k =0.65
- the sequence generated for N numbers
  - $\{X_k\}$ =$\{$0.819000, 0.533660, 0.895921, 0.335687, 0.802805, 0.569913, 0.882404, 0.373563,...$\}$
- calculate the arithmetic mean ,Threshold(T),of N real numbers
  - $T = {}^{N}\Sigma_{k=0} \; (x_k /N)$

    =0.646400 (for the above example)
- if x_k >= T then B_k =1 else B_k =0,where B_k is the encoded binary sequence generated

- N=8, μ=3.6, x_k =0.65, x_{k+1} =μ x_k (1- x_k), T=0.65162

- Chaotic sequence is as follows:

0.819000	**0.533660**	**0.895921**	**0.335687**	**0.802805**	**0.569913**	**0.882404**	**0.373563**
1	0	1	0	1	0	1	0

- Take 8 pixels of secret image. Let C_k =01010000,be 1 secret byte of secret image.

- First bit of binary sequence generated from chaos function $\mathbf{B}_{\mathbf{k}=1}$

- Convert to 8bit by adding 7 ones to left of $\mathbf{B}_\mathbf{k}$
➢ B_k =1111111*[1]*

- Perform XOR bet ret image is embedded with 1bit chaos)

C_k =01010000	
B_k =11111111	
C_k '=10101111	

CONSIDER LINEAR MAP FOR STEGANOGRAPHY

μ=3.6, X_k =0.65 Thus the sequence generate is

$X_{k=1,2,3}$ = {0.819000,0.533660,0.895921,0.335687,0.802805,0.569913,0.882404,0.373563}

Arithmetic mean=0.646400

Threshold T=0.646400

Encoding in binary is 10101010

jkm.cse@gmail.com

Selection of Insertion position

jkm.cse@gmail.com

Algorithm - Hash Map

1. A set of functions is used in the mutation process that needs to be generated a priori.

2. These functions generate XOR values as a function of the pixel coordinates.

3. This set of functions is the first key of the encryption process.

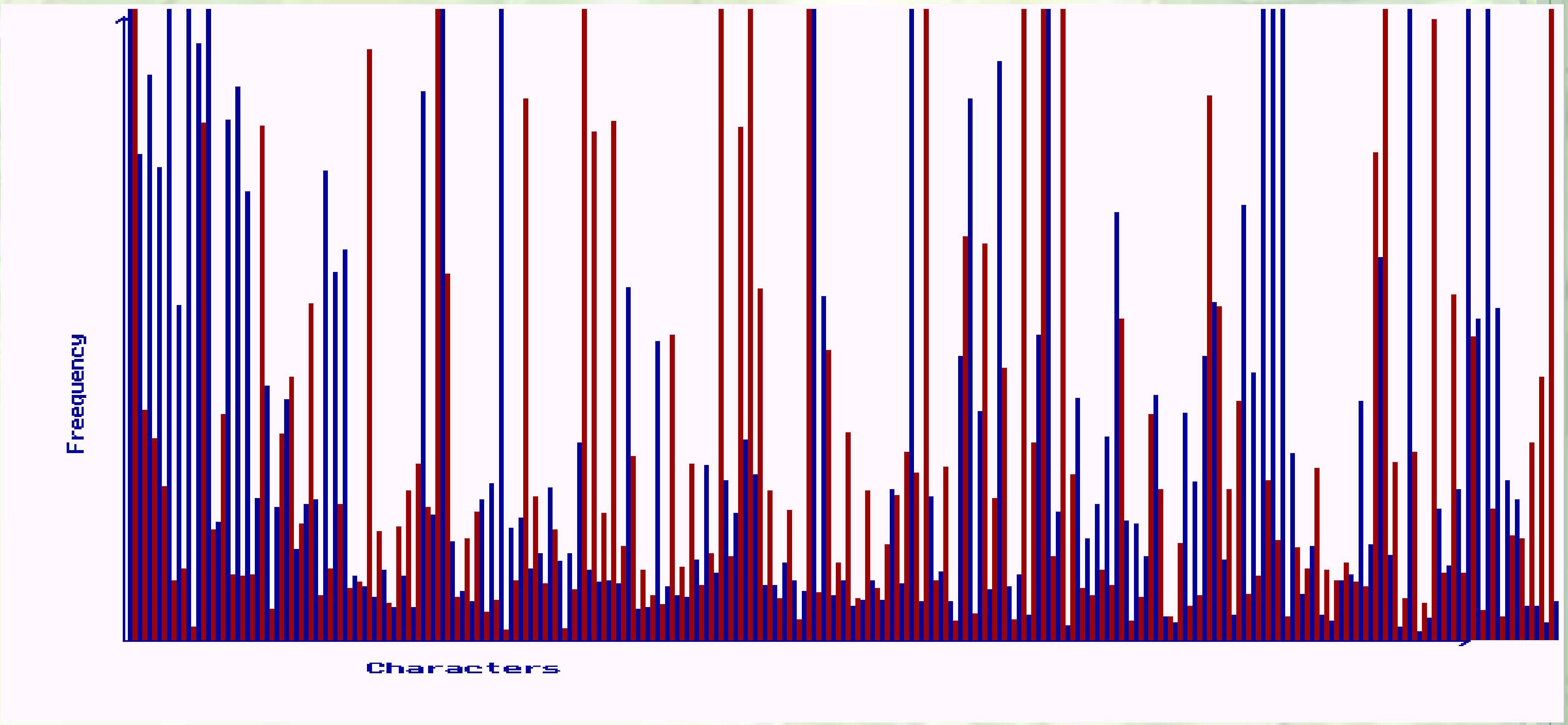
4. Each of these functions is uniquely identified by an integer, represented by the variable id.

Chromosome Representation

1. Each chromosome represents a possible solution, i.e., an encrypted image.

2. For a true color (24-bit) input image having height H and width W pixels the corresponding chromosome is a three dimensional matrix $W \times H \times 3$ with 8-bit entries in each of the three layers of red, green and blue, i.e., each layer consists of $W \times H$ pixels.

A SEGMENT OF FREQUENCY DISTRIBUTION FOR CHARACTERS IN TLIB.EXE AND ITS ENCRYPTED FILE

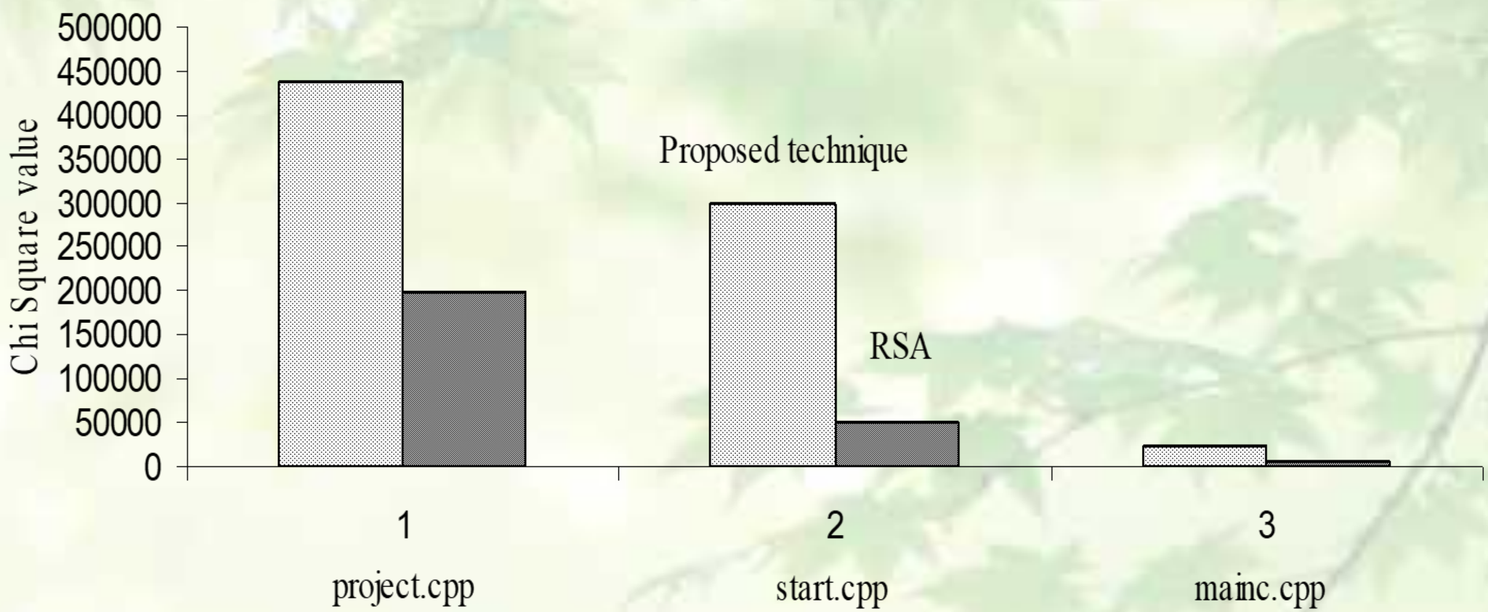


Blue lines indicate the occurrences of characters in the source file and red lines indicate the same in the corresponding encrypted file

Comparative results between RPMS technique and RSA technique for .cpp files for their Chi Square values and corresponding degree of freedom

Source file	Encrypted files using RPMS technique	Encrypted files using RSA technique	Chi Square value for RPMS technique	Chi Square value for RSA technique	Degrees of freedom
bricks.cpp	*a1.cpp*	*cpp1.cpp*	113381	200221	88
project.cpp	*a2.cpp*	*cpp2.cpp*	438133	197728	90
arith.cpp	*a3.cpp*	*cpp3.cpp*	143723	273982	77
start.cpp	*a4.cpp*	*cpp4.cpp*	297753	49242	88
chartcom.cpp	*a5.cpp*	*cpp5.cpp*	48929	105384	84
bitio.cpp	*a6.cpp*	*cpp6.cpp*	9101	52529	70
mainc.cpp	*a7.cpp*	*cpp7.cpp*	22485	4964	83
ttest.cpp	*a8.cpp*	*cpp8.cpp*	1794	3652	69
do.cpp	*a9.cpp*	*cpp9.cpp*	294607	655734	88
cal.cpp	*a10.cpp*	*cpp10.cpp*	143672	216498	77

Files with better result in proposed technique than existing RSA technique in terms of Chi Square values



Questions & Comments

jkm.cse@gmail.com

THANK YOU

Dr. Jyotsna Kumar Mandal

jkm.cse@gmail.com