IMAGE ENCRYPTION AND DECRYPTION USING A MASK AND RSA ALGORITHM

A PROJECT REPORT FOR J COMPONENT
NETWORK SECURITY (CSE 2008)

PROJECT SUPERVISOR
ANIL KUMAR K

Submitted by

NAME	REG NO.
NAVDEEP BENIWAL	16BCB0077
SAI TEJA	16BCI0209
PRIYA KUMARI	16BCI0211

School of Computer Science and Engineering

VIT®
UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ■ CHENNAI
www.vit.ac.in

MARCH 2018

CERTIFICATE

This is to certify that the project entitled, “**Image Encryption And Decryption Using A Mask And RSA Algorithm**" submitted by the students **Priya Kumari(16BCI0211), Navdeep Beniwal(16BCB0077), Sai Teja(16BCI0209)** for the course "**Network Security (CSE-2008)**" at “VIT university", is an authentic work carried out by them under my supervision and guidance. To the best of my knowledge, the matter embodied in the project has not been submitted to any other University / Institute for any purpose.

Date: 25-03-2018
Place: VIT University, Vellore
Signature

ACKNOWLEDGEMENTS

We would like to extend our thanks to the management of VIT University, Vellore and our respected chancellor G. Viswanathan for giving us the opportunity to carry out our project in VIT. We would also like to extend our gratitude to our faculty, Prof. Anil Kumar K for his constant and ceaseless guidance and support through the entire course of this project. We would also want to thank sir for guiding us all along the way and encouraging us to think out of the box in an attempt to maximize the project's validity for the society.

Navdeep Beniwaal(16BCB0077)
Sai Teja(16BCI0209)
Priya Kumari(16BCI0211)

ABSTRACT

In the recent world, security is a prime important issue; the need of information security has become a necessity with the progressing data exchange and communication by electronic system. Because of the growth of multimedia application, security becomes an important issue of communication, storage and transmission of data and encryption is one of the best alternative ways to ensure security. Moreover, there are many image encryption schemes have been proposed, each one of them has its own strength and weakness.

We propose a mixed algorithm for image encryption which employs the concept of masking the image. Mask is generated using key. Although it involves RSA algorithm to provide two level of security.

Here, the input will be a image in the form of matrix of size mxn. We will enter any text as a key. Similar to vignere cipher the key will repeat itself until it forms a matrix of size mxn. Any mathematical operation like addition, subtraction and multiplication can be performed on this two images, resultant will be a new image with size mxn. Then after applying RSA algorithm, we will get the final encrypted image.

Keywords-

1. Original image- image that is to be send during communication.
2. Mask- image that is generated using key_s(shared between sender and receiver)
3. Encrypted Imgae- image that hides real property of image inside it.

Table of Contents

1. Introduction 6
2. Description of the Algorithm 7
3. 5 out of 8 code 8
4. Code 10
5. Result 13
6.DisAdvantages 19
7. Applications 20
8. Conclusion 21

Introduction

Image encryption has application in internet communication, video conferencing, telemedicine, distance education through video on demand, multimedia system, military and satellite image processing and much othet application require information security.

We have proposed a novel technique for image encryption using concept of 5 out of 8 code in which mask is created with the help of alphanumeric password. This password is shared between both sender and receiver. Its a kind of symmetric key algorithm. Each alphanumeric character is assigned wit a unique 8 bit code where 8 bit consisting of 5 ones and 3 zeroes. By using this there is a possibility of constructing only 43 combinations of unique codes. 43 uniques codes are assigned to 26 alphabets, 10 numerals and 7 symbols. Using this code we had created a mask. This mask will get added to the original image which will produce a slight distorted image.

On mask , we will perform RSA algorithm. RSA algorithm is a assymetric method of encryption and decryption. In contrast to symmetric key algorithm it uses two different key public and private.

Encryption and Decryption Process in RSA

- Choose two large distinct primes p and q and then form the public modulus n = pq.
- Calculate phi(n)=(p-1)(q-1)
- Choose public exponent e to be coprime to phi(n), with $1 < e < phi(n)$.
- The pair (n, e) is the public key.
- The private key is the unique integer $1 < d < phi(n)$ such that $ed = 1 \bmod phi(n)$.

Encryption:

Split a message M into a sequence of blocks M1, M2, . . . , Mt where each Mi satisfies $0 \leq Mi < n$.
Then encrypt these blocks as: $C=M^e \bmod n$

Decryption:

Given the private key d and the ciphertext C, the decryption function is:$M=C^d \bmod n$

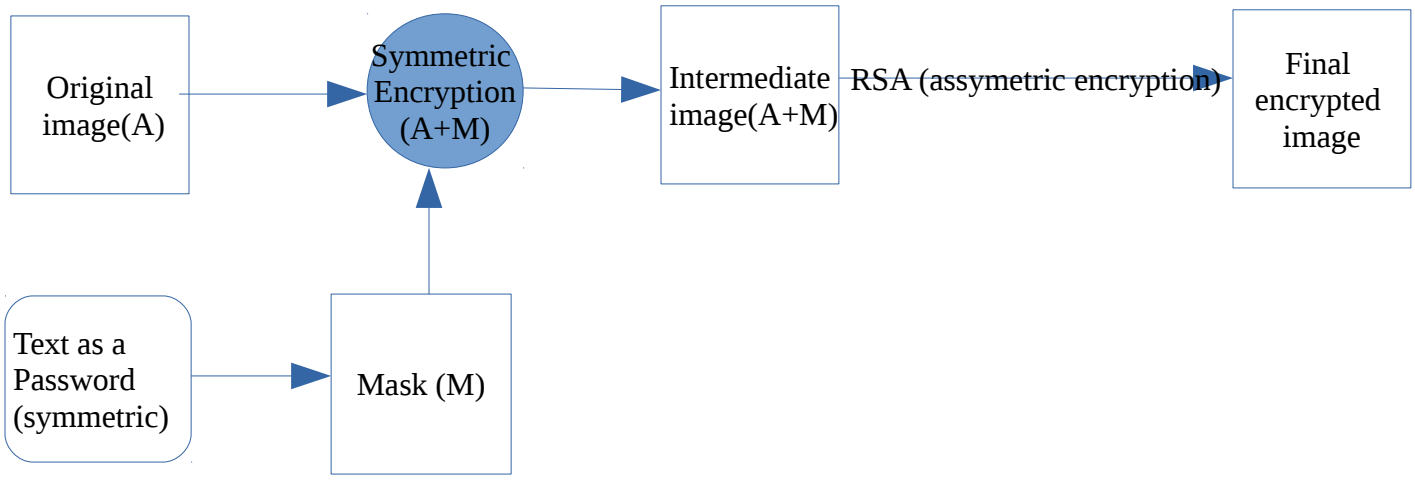
NOTE-

- Encryption does not increase the size of a message. Both the message and the ciphertext are integers in the range 0 to n – 1.

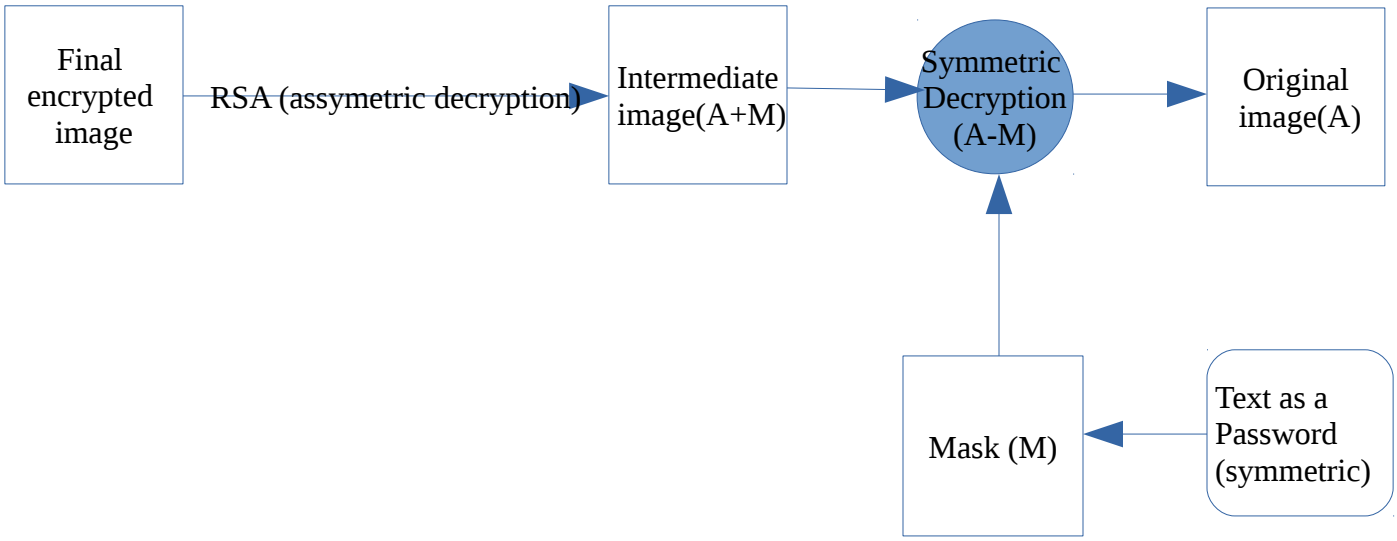
- The encryption key is thus the pair of positive integers (e; n). Similarly, the decryption key is the pair of positive integers (d; n). Each user makes his encryption key public, and keeps the corresponding decryption key private.

DESCRIPTION OF THE ALGORITHM

Encryption Process



Decryption Process



5 Out Of 8 Code

S NO.	BINARY	DECIMAL	ALPHANUMERIC
1	00011111	31	A
2	00101111	47	B
3	01001111	79	C
4	01010111	87	D
5	01011011	91	E
6	01011101	93	F
7	01011110	94	G
8	01100111	103	H
9	01101011	107	I
10	01101101	109	J
11	01101110	110	K
12	01110101	117	L
13	01110110	118	M
14	01111001	121	N
15	01111100	124	O
16	10001111	143	P
17	10010111	151	Q
18	10011011	155	R
19	10011101	157	S
20	10011110	158	T
21	10100111	167	U
22	10101011	171	V
23	10101101	173	W
24	10101110	174	X
25	10110101	181	Y
26	10110110	182	Z
27	10111001	185	1

28	10111100	188	2
29	11000111	199	3
30	11001011	203	4
31	1100101	205	5
32	11001110	206	6
33	11010101	213	7
34	11010110	214	8
35	11011001	217	9
36	11011100	220	0
37	11100101	229	@
38	11100110	230	#
39	11101100	236	$
40	11110001	241	%
41	11110010	242	&
42	11110100	244	!
43	11111000	248	*

CODE

```
tic
Pattern=['00110011';
         '00110101';
         '00110110';
         '00111001';
         '00111010';
         '00111100';
         '01010011';
         '01010101';
         '01010110';
         '01011001';
         '01011010';
         '01011100';
         '01100011';
         '01100101';
         '01100110';
         '01101001';
         '01101010';
         '01101100';
         '10010011';
         '10010101';
         '10010110';
         '10011001';
         '10011010';
         '10011100';
         '10100011';
         '10100101';
         '10100110';
         '10101001';
         '10101010';
         '10101100';
         '11000011';
         '11000101';
         '11000110';
         '11001001';
         '11001010';
          '11001100']
Chars=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p
','q','r','s','t','u','v','w','x','y','z','0','1','2','3','4','5','6'
,'7','8','9'];
pw=input('Enter a password:');
[fname path]=uigetfile('*.jpg','enter the image');
fname=strcat(path,fname);
im=imread(fname);
img=im;
imshow(im);
title('actual image');
```

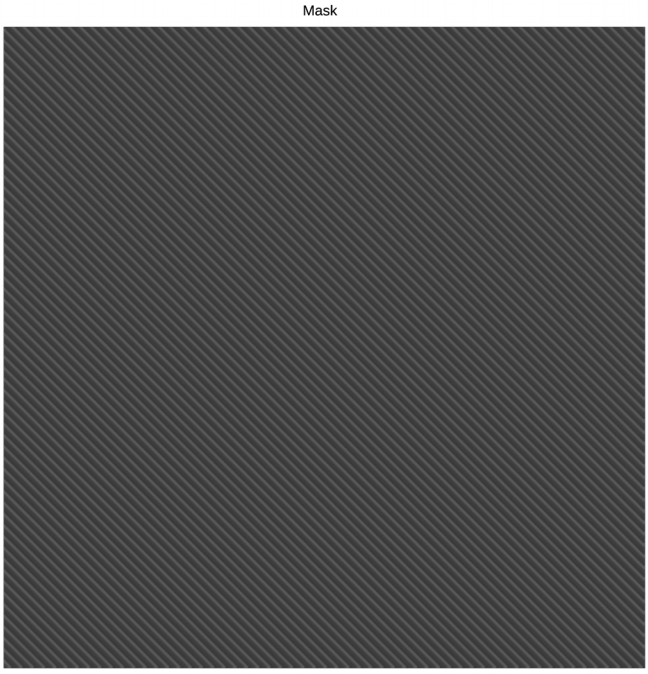
```
[x y z]=size(im);
for(i=1:length(pw))
    a=pw(i);
    a=find(Chars==a);
    a=Pattern(a,:);
    num(i)=bin2dec(a);
end

k=1;
for(i=1:x)
   for(j=1:y)
       car(i,j)=num(k);
       k=k+1;
       if(k>length(num))
          k=1;
       end
   end
end
figure;
imshow(uint8(car));
title('Mask');

im=double(im);
for(i=1:z)
    im(:,:,i)=im(:,:,i)/10;
end

for(i=1:z)
   A=im(:,:,i);
   A=A+car;
   im(:,:,i)=A;
end
figure;
imshow(uint8(im));
title('Encrypted image');
[x1 y1 z1]=size(im);
for i=1:x1
    for j=1:y1
       P(i,j)= mod((im(i,j)^5),1649);
   end
end
figure;
imshow(P);
title('rsa encrypted image');
[x1 y1 z1]=size(P);
for i=1:x1
    for j=1:y1
       im(i,j)= mod((P(i,j)^1229),1649);
   end
```

```
end
for(i=1:z)
P=im(:,:,i);
P=P-car;
im(:,:,i)=P*10;
end
figure;
imshow((img));
title('Decrypted image');
toc
```

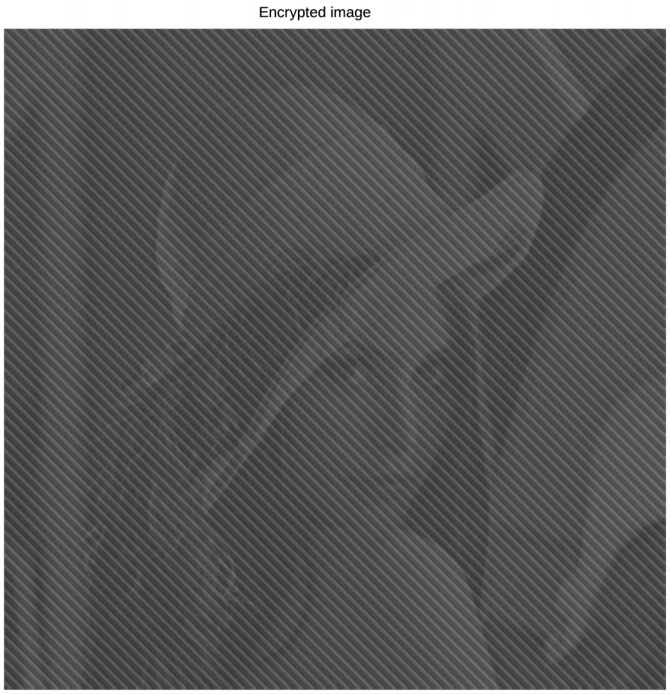
RESULT

1. key= ‘abcdefghi’
actual image-

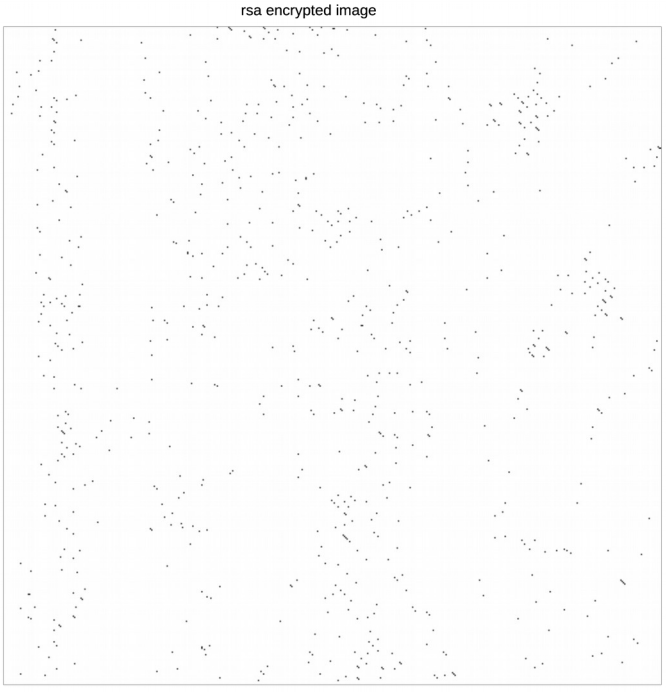
mask-



encrypted image= original image + mask



rsa encrypted image= RSA(encrypted image)



Decrypted image

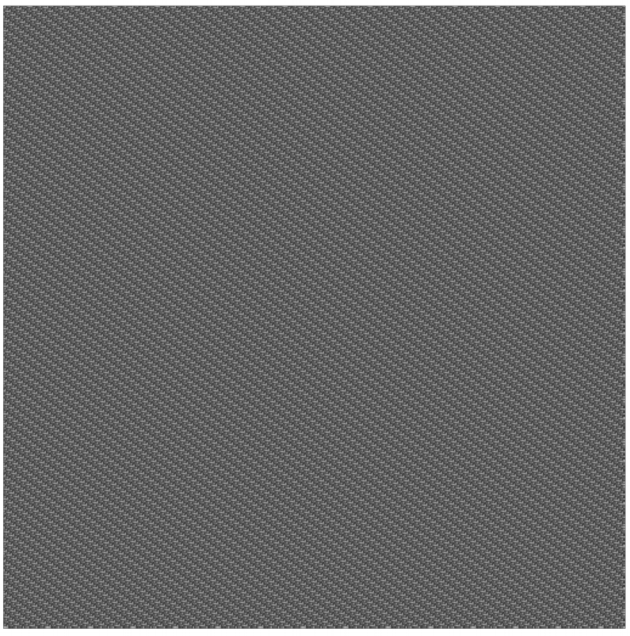
computational time=13.957 seconds

2. key=’sdfghjkwertyuixcvbnmstyucvbnm’
actual image-

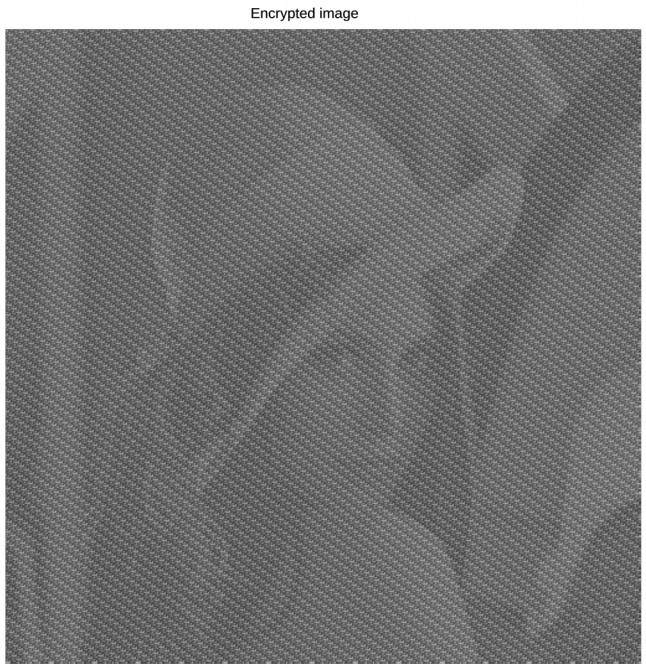
actual image

mask

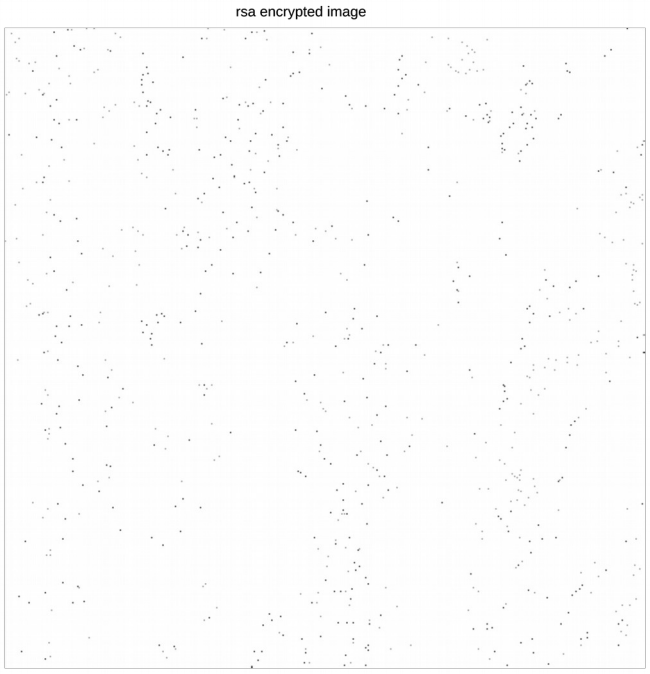
Mask



encrypted image= original image + mask



rsa encrypted image= RSA(encrypted image)



Decrypted image

Decrypted image

computational time- 33.64 seconds

DIS-ADVANTAGES

- As the length of key, computational time increases.
- Small keys are easy to break and does not hide information in image more effectively.
- Value of elected prime number for RSA algorithm also determines the secured level of image.

APPLICATIONS

- internet communication
- social networking sites
- video conferencing
- telemedicine
- distance education through video on demand
- multimedia system
- military image processing
- satellite image processing

CONCLUSION

- As the size of symmetric key increases, more complex mask is formed. We can see and compare the mask in both cases.
- As the length of key, computational time increases.
- Value of elected prime number for RSA algorithm also determines the secured level of image.
- Small keys are easy to break and does not hide information in image more effectively.
- In case if someone intercepts the encrypted image, it is very hard to get decrypted image as two level of security is defined on encrypted image. One using mask and another applying RSA algorithm on intermediate encrypted image.
- Symmetric key contains alphabet, number and special character. It is easy to find out symmetric key by unauthorized party as ASCII value of these characters are known to every one. So we have defined our own pattern . We assigned different numerical value to every character. For example ASCII value of ‘a’ is 97 but we had given it as ‘31’. This method will make harder for a hacker to know the exact key value.
- It is suggested to use random character like ‘sdfgwerthcvbn’ in key instead of using continuous character like ‘abcd’. Beacuse random character produces more complex mask .