iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5360

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Study and Analysis of RSA Algorithm using Iris for Data Security

Pooja Kallolimath[1], Dr. Prashant P. Patavardhan[2]
[1, 2]*Department of Electronics and Communication, KLS Gogte Institute of Technology, Belgaum, India*

Abstract: ***In biometrics, every individual must be identified based on some characteristic physiological parameters. A wide variety of recognition schemes are used to either determine or confirm the identity of an individual requesting their services. In the proposed work, different modules are combined to generate more secure cryptographic key from iris image. In the initial stage, iris images from the CASIA Database V1.0 are processed to locate the iris region and this region is normalized into a dimensionally constant rectangular block using Daugman's operator know as rubber sheet model. Principal component analysis is used to match the rubber sheet models. Two unique prime numbers have been assigned for the selected portion of the rubber sheet model which is to be utilized for the data encryption and decryption tasks. Most public-key cryptographic algorithms require the generation of random prime numbers. A naive solution to obtain a prime number consists of randomly choosing a number and testing it for primality. The generation of prime numbers underlies the use of most public-key cryptosystems, essentially as a primitive needed for the creation of RSA key pairs. Accuracy of the data encryption and decryption algorithm depends on the iris image segmentation. The algorithm was applied for 105 images of CASIA database and iris segmentation is approximately 85.71% i.e. 90 out of 105 images are segmented successfully.***
Keywords: Iris Recognition, RSA algorithm, Encryption, Decryption

I. INTRODUCTION

Use of Internet is growing rapidly. So providing security to the information over networks has become a crucial issue these days. Information should be disclosed solely to the intended recipient. In the network, information is more open to attacks. Cryptography techniques are used to prevent the sensitive information from the intruder. Encryption converts the original messages into coded messages by making a system immune to different attacks. At present, the best well-known and generally used public key cryptosystem for secure data transmission is RSA. In such a cryptosystem, the encryption key differs from the decryption key which is kept secret. This asymmetric algorithm is based on the practical factoring of the product of two large prime numbers. These prime numbers must be kept secret. Anyone can use the public key to encrypt a message but only with knowledge of the prime numbers one can possibly decode the message.

Biometric methods that are based on the every individual verification and identification processes are gaining additional interest in today's era because of rapid growth in the technology and high requirement for security. Among different biometrics like fingerprint, face recognition, iris and ear, iris recognition method is more accurate and reliable due to its unique statistical characteristic and high identification rate. These systems can be divided into two stages, enrolment stage and verification stage. In enrolment stage, eye images are captured using high quality camera and these eye images are pre-processed and the corresponding iris templates are stored in the database. In verification stage, user asks to submit their samples first, these templates are compared against the stored database and then decision is taken based on the threshold value. Basically a system is to be implemented to provide security to data using iris image stored in CASIA database. There is an essential need for personal characteristics based identification due to the fact that it can provide the highest protection against impersonation. This system consists of an image segmentation which detects the circular iris region, occluding eyelashes and eyelids and reflections. Along with this RSA algorithm is designed using iris template as key. The encryption and decryption processes work separately in combination with a key to encrypt and decrypt the data. The encrypted data security totally depends on the confidentiality of the key.

II. RELATED WORK

Mahajan et al. [2] discussed three algorithms Data Encryption Standard, Advanced Encryption Standard and Rivest Shamir Adleman algorithm. Data Encryption Standard and Advanced Encryption Standard are symmetric key cryptographic algorithms and Rivest Shamir Adleman is an asymmetric key cryptographic algorithm. Based on throughput, capability to secure information and time taken to encrypt data, these three algorithms are analysed and performance was different according to the inputs. It was

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

concluded that confidentiality and scalability provided by Advanced Encryption Standard over Data Encryption Standard and Rivest Shamir Adleman algorithm is much higher and makes it suitable.

Zhou et al. [3] discussed a most common encryption algorithm known as Rivest, Shamir and Adleman algorithm with the real fact that it's very difficult to factorize big integers. It is the first asymmetric cryptosystem which can be used in both key exchange and digital signatures. It has block size of 128 bits and key size varies from 1024 to 4096. Two different keys are utilized for encoding and decoding the data. It makes use of two prime numbers to generate public and private keys based on mathematical calculations and multiplying those large numbers together.

J.Daugman [6] designed and patented the first complete, commercially available phase-based iris recognition system in 1994. The eye images with resolution of 80-130 pixels iris radius were captured with image focus assessment performed in real time. The iris and pupil boundaries are detected using integro-differential operator. The centre coordinates and radius are estimated for both pupil and iris regions by determining the maximum partial derivative of the contour integral of the image along the circular arc. The iris portion of the image is normalized. Each pixel in the normalised iris pattern corresponds to two bits of data in the iris template. The representation of iris texture is binary coded by quantizing the phase response of a texture filter using quadrature 2D Gabor wavelets into four levels. This algorithm achieves high performance in iris recognition.

Masek [7] designed an open iris recognition system for the verification of human iris uniqueness and also its performance as the biometrics. The iris recognition system consists of an automated segmentation system, in which iris region is isolated from the original eye image using circular Hough transform.. By applying Daugman's rubber sheet model the segmented iris region converted into flexible rubber sheet rectangular block. Ultimately, the iris features were encoded by convolving the normalized iris region with the 1D Log-Gabor filters and phase quantizing the output to produce a bit-wise biometric template.

III.PROPOSED ALGORITHM

A. RSA Algorithm

RSA algorithm is the first public key cryptosystem that is widely used for secure data transmission which provides both secrecy and digital signature. It refers to the name of its discoverers, Ron Rivest, Adi Shamir and Len Adelman in 1977. In this algorithm two unique prime numbers are used to produce public key and private key. It basically involves three steps - key generation, encryption and decryption.

1) Key generation

a) Select two prime numbers P & Q.

b) Calculate $N = P \times Q$

c) Calculate $\Phi(N) = (P-1) \times (Q-1)$

d) Choose an integer E such that, GCD $[\Phi(N), E] = 1$

e) Determine $D = E^{-1} \bmod (\Phi(N))$

f) Public key ; PU = {E, D}

g) Private key ; PR = {D, N}

2) Encryption

a) Plain text : $M < N$

b) Cipher text : $C = M^E \bmod N$

3) Decryption

a) Cipher text : C

b) Plain text : $M = C^D \bmod N$

c) For example,

i) If P = 11 and Q = 17

ii) Then $N = P \times Q$

$= 11 \times 17$

$N = 187$

iii) Compute $\Phi(N) = (P - 1) \times (Q - 1)$

$= (11-1) \times (17-1)$

$= 10 \times 16$

$\Phi(N) = 160$

iv) Choose an integer E such that $1 < E < \Phi(E)$, E and $\Phi(N)$ are co-prime.

v) Let E = 13

vi) Determine $D = E^{-1} \bmod (\Phi(N))$

$= 13^{-1} \bmod (160)$

D = 37

vii) Public key (E, N) = (13, 187)

viii) Private key (D, N) = (37, 187)

ix) Encryption : If M = 20 then ,

$C = M^E \bmod N$

$C = 20^{13} \bmod 187$

C = 80

x) Decryption : C = 80 then,

$M = C^D \bmod N$

$M = 80^{37} \bmod 187$

M = 20

B. Generation of Random Prime Numbers

Prime numbers are randomly generated by considering a random number and checking it with AKS or MR primality property with applications to a variety of cryptography areas.

1) Generating primes using Goldbach Partitions: Goldbach Prime Generating Algorithm(GPGA) can be used as an alternate method in public key cryptography and in authentication techniques. The GPGA method has reduced the number of trials in the search for primes by a factor of nearly 10 for primes ranging from 45 to 70 digits long. Considering *g(n)* as a unique number and *n* is written as p + q, where p and q are two prime unique numbers.

For example,

If *n*=30 then the Goldbach partitions are (23, 7), (19, 11) and (17, 13).

If *n*=210 then the Goldbach partitions are (199,11) (197,13) (193,17) (191,19) (181,29) (179,31) (173,37) (167,43) (163,47) (157,53) (151,59) (149,61) (139,71) (137,73) (131,79) (127,83) (113,97) (109,101) (107,103).

2) Linear Sieve algorithm for finding prime numbers: A Linear Sieve algorithm is a fast method for determining all the prime numbers within a given range. It gives prime numbers by repeatedly marking all the composite numbers which are the multiples of each prime, starting with 2. The multiples of a given prime number are generated as a sequence of numbers ranging from that prime. It makes use of trial division technique to serially check each number for divisibility by each prime. The Sieve's algorithm is a best way to determine all the prime numbers smaller than any given natural number.

For example,

If *n*=20, then the prime numbers are "2, 3, 5, 7, 11, 13, 17 and 19".

If *n*= 50, then the prime numbers are " 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47"

A Linear Sieve algorithm is as follows,

a) Make a list of successive integers from 2 to *n*.

b) et *x* =2, be the 1st prime number

c) Increase the value of *x* for every iteration and mark the numbers which are greater than *x* within the list. The numbers will be 2*x*, 3*x*, 4*x*, etc. and note that few of these numbers have already been marked in previous iterationsIn the next iteration select the number greater than *x* which is not marked in the list. If all the numbers have been marked in the list and then terminate. Otherwise, now *x* equals to the next prime number and repeat the step 3. When the algorithm stops, all the numbers which are not marked in the list are prime numbers.

3) Primes and Twin Primes Generator Algorithm: Primes and Twin Primes generator algorithm is based on the divisibility properties of binomial expressions. The mathematical connection exists between binomial expressions and the number of carries that lead to the sum in different bases of the variables that form the binomial expression. The first part decomposes an integer into its prime factorization and generates the prime numbers, while the second part checks whether the given two prime integers are twin primes or not by just verifying the condition.

For example,

If *n* = 15 then the twin prime pairs are (3,5) (5,7) and (11,13).

4) Primes and twin primes generator algorithm :

a) Enter x and y.

b) If y is a prime then $3 < y \leq 2x + 1$.

c) If the number of carries is C >1, then pair $(2x - 1, 2x + 1)$ is a twin prime integer in the set y else it is not a twin prime pair. Then y divides either $2x-1$ or $2x+1$.

d) In next iteration select $x = x + 1$ and repeat step 2 & 3.

4) Constructive Methods for the Generation of Prime Numbers

One of the simple method to generate prime number is to select any random integer x and testing it for primality property, if it is not successful then repeat the algorithm with $x = x + 1$. Except 2, all the other prime numbers are odd. An improvement is to select x odd and to update x as $x = x + 2$. This is a method, where a selected number x is coprime to many other small primes.

For example,

If $q = 20$, the output will be "2, 3, 5, 7, 11, 13, 17, 19".

If $q = 70$, the output will be " 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67"

5) Algorithm for the generation of prime numbers :

a) Select any random integer x

b) If $T(x)$ = false then go to step 1

c) output x.

C. Iris Recognition Method

Success of the system is directly proportional to the quality of the images. Low quality and noisy images decrease the performance of the system. In the CASIA iris database, near infra-red light is used to avoid specular reflections. The CASIA Database Version 1.0 also referred as 'CASIA Iris V1' contains 756 iris images from 108 eyes. All the pictures are stored as BMP format with resolution 320*280. The steps involved in the iris recognition method is as shown in Fig. 1.

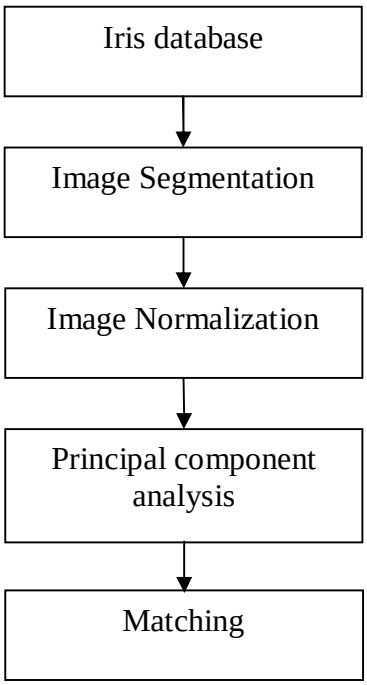


Fig.1. Iris Recognition Flow

1) Image Segmentation: In iris recognition method, first step is to separate the actual iris region in original eye image. The iris region is separated by two circles, one is the limbus or sclera boundary and another one is iris/pupil boundary. The upper and lower

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

parts of the iris region are normally covered by eyelids and eyelashes. A technique is required to isolate and eliminate these artifacts as well as locating the circular iris region. An integro-differential operator is used for detecting the iris and pupil areas. The Daugman's integro-differential operator is defined as,

$$\max_{(r,xp,yo)} = \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,xo,yo} \frac{I(x,y)}{2\pi r} ds \right| \quad \text{eq. (1)}$$

where,

I(x,y) → Eye image.
r → Radius to search.
$G_\sigma(r)$ → Gaussian smoothing function.
s → Contour of the circle given by r, x_0, y_0.

The operator creates a circular path by changing the radius *r* and centre *x* and *y* position if there is a maximum change in the pixel values. This process is repeated in order to attain precise localization.

2) Image Normalization: After segmenting the iris part from an eye image, the second step is to convert this iris area into rectangular form with fixed dimensions in order to allow comparisons. Irregularities in the dimensions are caused by the stretching of the iris which leads to the errors in the calculations. This is done using Daugman's rubber sheet model, where each point in the iris area is remapped into polar coordinates (r,θ) as shown in Fig. 2.

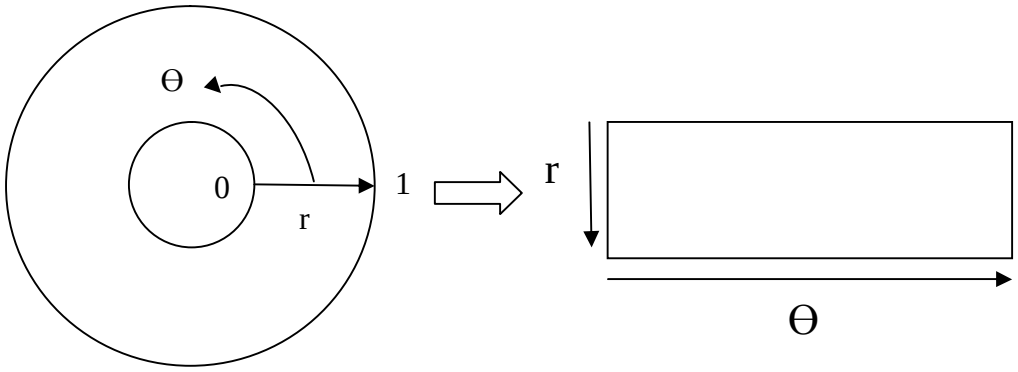


Fig. 2. Daugman's Rubber sheet Model

The iris region is remapped from Cartesian coordinates to normalized polar coordinates which is represented as,

$$I(x(r,\Theta), y(r,\Theta)) \longrightarrow I(r,\Theta) \quad \text{eq. (2)}$$

with

$$x(r,\Theta) = (1-r)\, x_p(\Theta) + r x_l(\Theta)$$
$$y(r,\Theta) = (1-r)\, y_p(\Theta) + r y_l(\Theta)$$

where,

I(x,y) → Iris region.
(x,y) → Original Cartesian coordinates.
(r,θ) → Normalized polar coordinates.
(x_p, y_p) & (x_l, y_l) → Coordinates of the pupil and iris boundaries along the θ direction.

3) Principal Component Analysis: Principal Components Analysis (PCA) is a data transformation technique invented by Karl Pearson in 1901. This technique is very popular in the fields such as image compression and face recognition. If a number of variables are to be measured for a series of objects or persons, then each variable will have a variance. These variables are related each other i.e. there will be covariance between pair of variables. The data set used for recognition as a whole will have a total variance which is the sum of the individual variances. 105 iris images from the CASIA database are selected, obtained two dimensional iris template is converted into one dimensional template.

The steps involved in PCA are listed below :

a) Get an image dataset of size m x n.

b) Calculate mean of the image.

$m = \sum_{n=0}^{N} Tn$ eq. (3)

where,

N = Total number of registered iris templets.

T = Training data set.

c) The mean is subtracted from each pixel of the image to get a zero mean vectors set Ai and is given by,

$A_i = T_i - m$ eq. (4)

where,

i - Ranging from 0 to N.

Ti - Training data set of N images.

d) Compute the co-variance matrix A.

$C = [A_i]^T * A_i$ eq. (5)

e) Calculate Eigen values and Eigen vectors .

$[C-\lambda I]\ e = 0$ eq. (6)

where,

λ - Eigen value.

e - Eigen vector.

I - Identity matrix with N eigen vectors.

f) These Eigen vectors are multiplied with set of zero mean vector Ai to form a feature vector.

$f_i = [A_i] * e_i$ eq. (7)

4) Matching: Euclidean distance is used match the eye images. The distance between the test images with a derived feature vectors in the training dataset are measured. Certain threshold value is set to reject or accept the images in the training data set. Images with greater value than the threshold value are neglected. The Euclidean distance is calculated as follows,

$E_k = \| f - f_k \|^2$ eq. (8)

IV. RESULTS

A. RSA Algorithm

RSA is a strong cryptographic technique which can be used to encrypt and decrypt any given data. The algorithm asks user to enter the two prime numbers P & Q, then it calculates the value of N, Φ ,E & D. After generating the public and private keys it asks user again to provide input data that is to be encrypted. The encryption and decryption results for a given data is as shown Fig. 3.

```
Command Window
RSA Algorithm Implementation
ENTER A PRIME NUMBER VALUE FOR P :
11
ENTER A PRIME NUMBER VALUE FOR Q :
17

THE VALUE OF N IS : 187
THE VALUE OF Pi(187) is : 160
THE VALUE OF E co-prime to Pi(n) is : 13
THE VALUE OF D is : 37

GENERATED Public Key Set is (13,187)
GENERATED Private Key Set is (37,187)

Provide Input Message to be Encrypted :
Hello User 123 !
ASCII Value of Input Message is :
    72   101   108   108   111    32    85   115   101   114    32    49    50    51    32    33


The Encrypted Message in ASCII is
    106 118 146 146 144 87  17  81  118 31  87  70  84  68  87  33
The ENCRYPTED MESSAGE IN STRING FORMAT IS

ans =

jv'' W Qv WFTDW!


The Decrypted message  in ASCII is
    72  101 108 108 111 32  85  115 101 114 32  49  50  51  32  33
The Decrypted Message in String is:

Hello User 123 !
```

Fig. 3. RSA Encryption and Decryption

B. Generation of Prime Numbers

The prime numbers are generated using Goldbach partition method. The algorithm asks user to give any even natural number greater than 2 and then displays all the primes within that range. For a given natural even number 100, the results are as shown in Fig. 4.

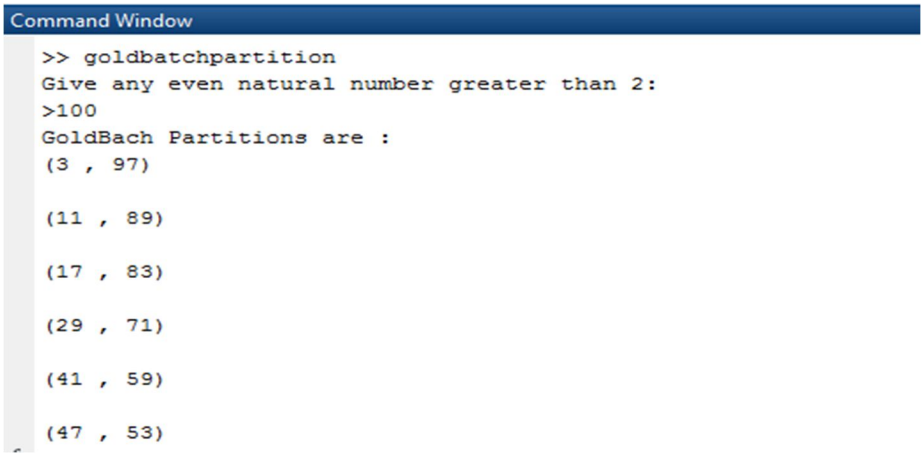


Fig. 4. Goldbach Partition Algorithm

Linear Sieve algorithm is a fast method for finding all the prime numbers within a given range. It gives prime numbers by repeatedly marking all the composite numbers which are the multiples of each prime, starting with 2. For a given maximum limit 60, the generated prime numbers are as shown in Fig. 5.

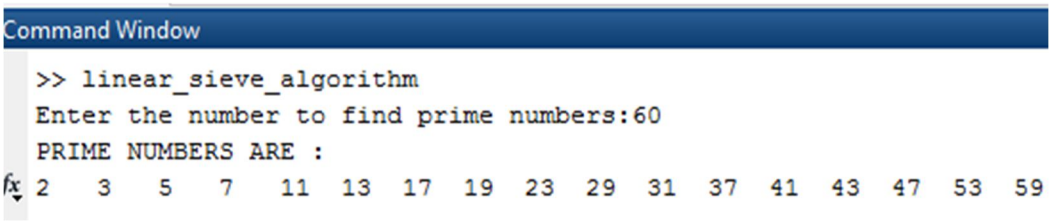


Fig. 5. Linear Sieve Algorithm

A prime number is twin prime if the difference between them is 2 i.e. a prime number is either 2 more or 2 less than the other prime number. The twin prime generator algorithm generates all the twin primes within a given range. For the given value 50, the generated prime numbers are as shown in Fig. 6.

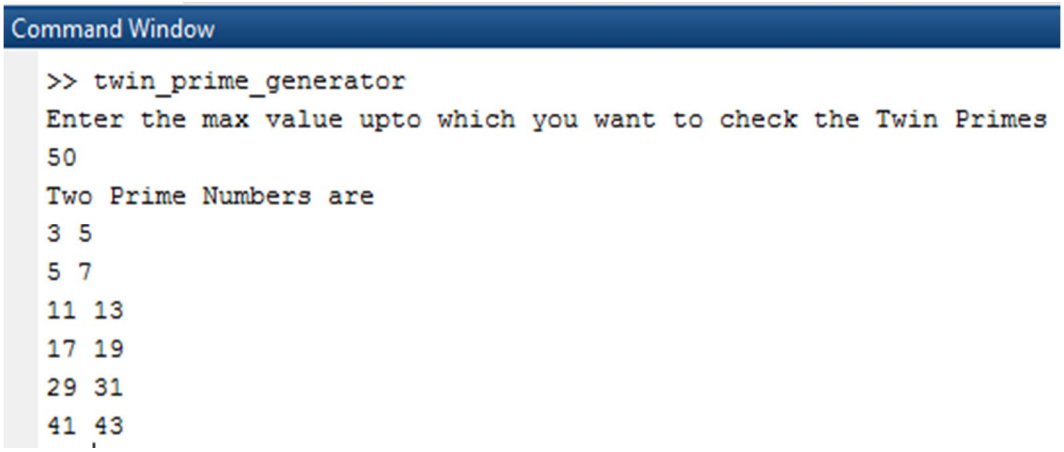


Fig. 6. Twin Prime Generator Algorithm

Another simple method is presented for generating the prime numbers within a given maximum range. For the given range 40, the generated prime numbers are as shown in Fig. 7.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

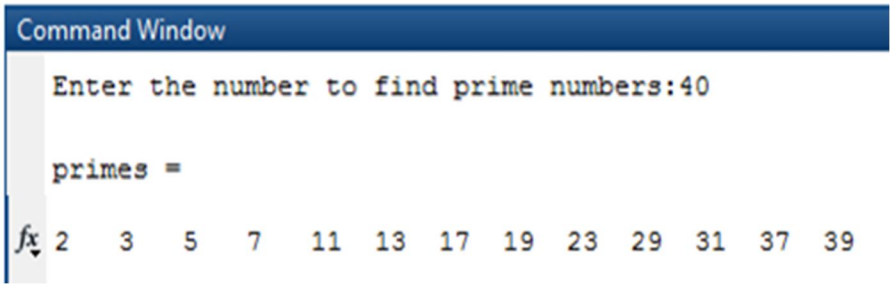


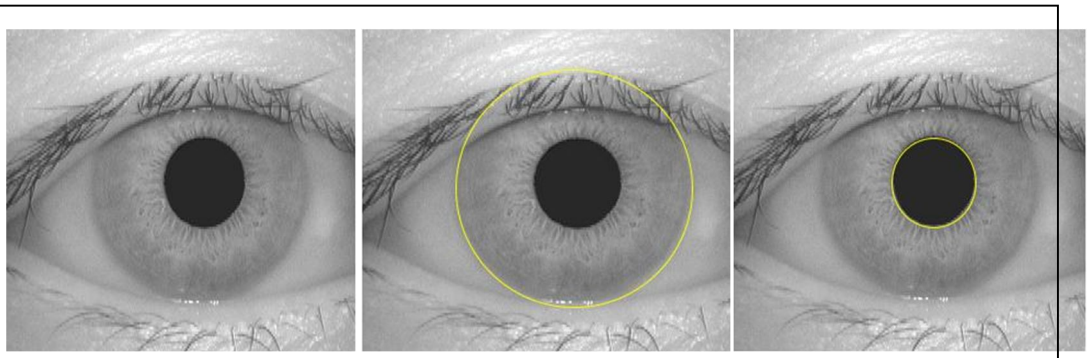
Fig. 7. Constructive Algorithm

C. Iris Recognition Method

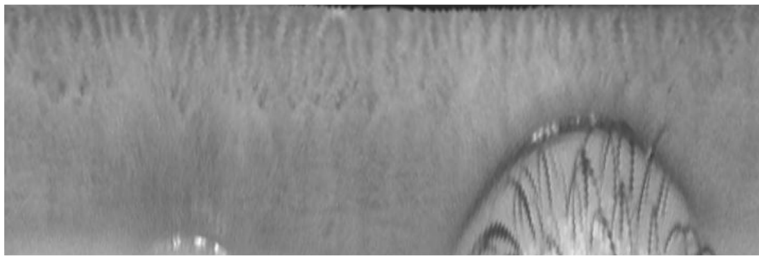
The iris images are taken from CASIA Iris Database Version 1.0. The advantage of using this database is because of its high quality images which do not possess specular reflections. 105 eye images from 20 different persons are considered where every person has 7 images captured in different conditions.

In iris recognition method, to separate the iris region from the original image (a), Daugman's integro-differential operator is used where outer boundary (b) and inner boundary (c) of iris region are detected. This circular iris region is converted into rectangular form using Daugman's rubber sheet model (d) in order to allow comparisons as shown in Fig. 8.

Next this rubber sheet model is divided into two halves i.e. left (e) and right (f) portions. Only left part of it is considered for further calculations neglecting the eyelid and eyelash portion to avoid error in the calculations. For the selected part two unique prime numbers have been assigned and saved in separate training data set. This iris recognition process is carried out for all the 105 eye images and left portion of rubber sheet model with assigned prime number is saved in training data set for identification purpose.



(a) Original Image (b) Outer Edge Detection (c) Inner Edge Detection



(d) Rubber sheet Model

(e) Left portion of rubber sheet model

(f) Right portion of rubbers sheet model

Fig. 8. Segmentation and Normalization process

D. Modified RSA Algorithm

In RSA encryption part, any eye image from the CASIA database is selected. Then the iris segmentation and normalization processes are carried out. Once the rubber sheet model is obtained, the left portion of it to which prime numbers have been assigned is selected. These prime numbers are used as input to the RSA algorithm. PCA algorithm is applied to identify which eye image has been selected for the encryption process from the training database by comparing the rubber sheet models. Suppose a different image is selected for the encryption process which is not there in the training data set, then with the help of Euclidean distance, PCA verifies all the rubber sheet models of eye images in the training data set and the image with smaller distance is considered for the further calculations.

Fig. 9. RSA Encryption Process

The prime numbers P & Q are selected from the left part of rubber sheet model, then it calculates the values of N & Φ. After generating the private and public keys it asks user to enter the message that is to be encrypted. This encrypted message is stored in MATLAB file known as "encrypted_mesg" file as shown in Fig. 9.

In RSA decryption part, different eye image of a same person is selected from the CASIA database. Then the iris region segmentation and normalization processes are carried out. Once the rubber sheet model is obtained, the left portion of it to which prime numbers have been assigned is selected. These prime numbers are used as input to the decryption part.

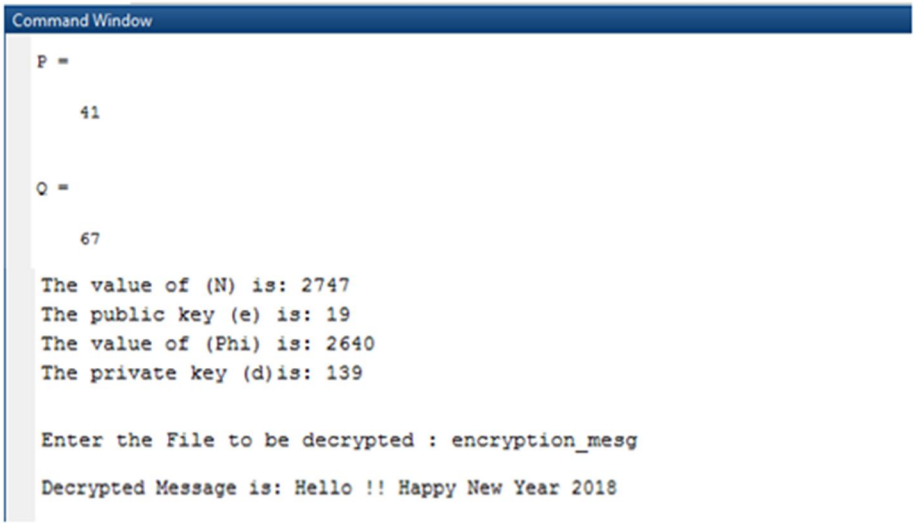


Fig. 10. RSA Decryption Process

The prime numbers used in this process should be same as that of the encryption process, then it calculates the values of N & Φ. After generating the private and public keys it asks user to enter the file in which the encrypted message is stored. The decrypted message is as shown in above Fig. 10 , which is same as the input message.

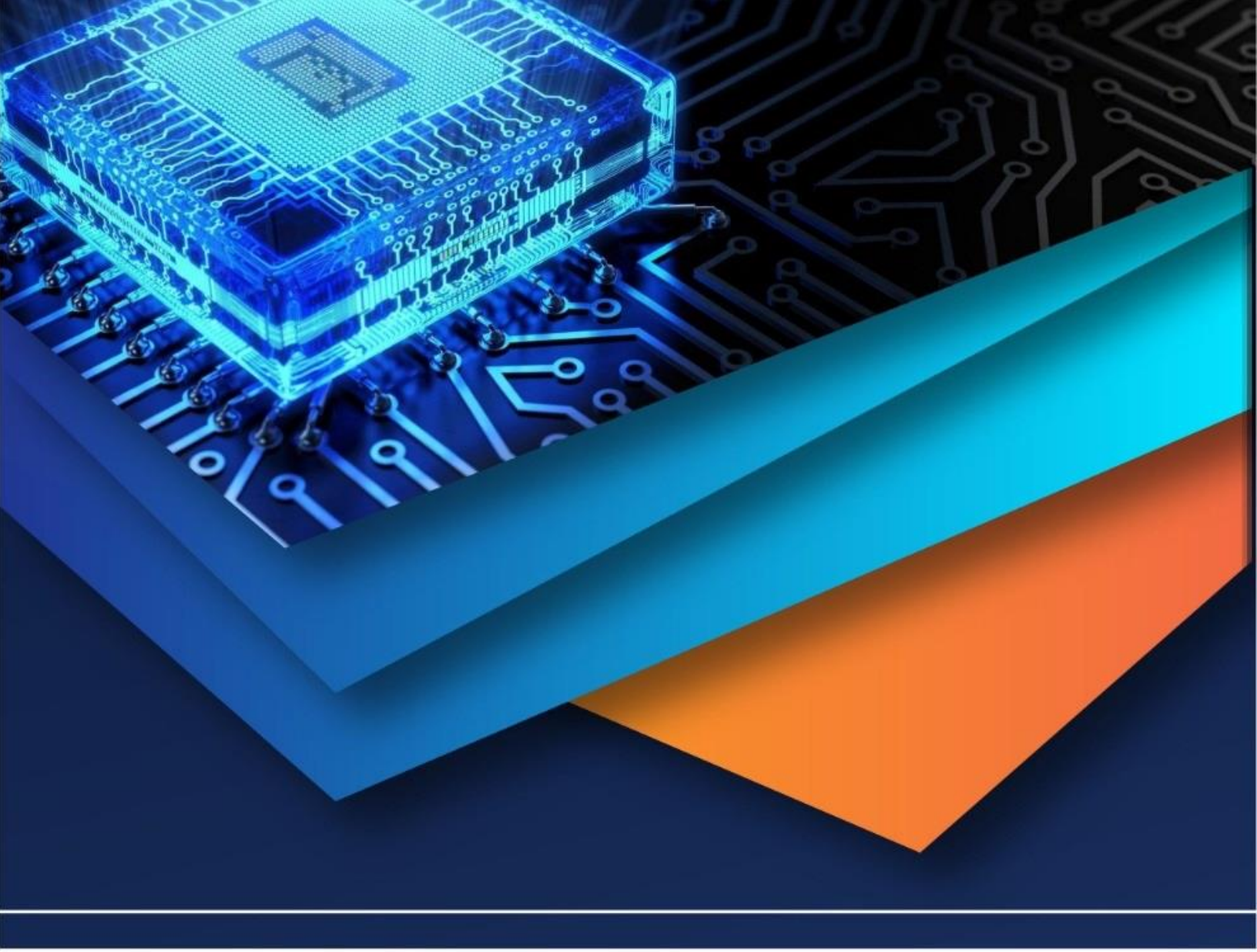
In this algorithm, two separate images of a same person are used for encrypting and decrypting of a given data. This method will be successful only if the iris image segmentation and matching is done appropriately. Otherwise, for a given data encryption and decryption processes will be failed. Segmentation is a main step in iris recognition, because the part which is wrongly identified as iris will corrupt the iris templet resulting in poor recognition. So accuracy of the algorithm for segmentation is approximately 85.71% i.e. 90 out of 105 images are segmented successfully.

V. CONCLUSION

With the rapid growing of internet and networks applications, security of information becomes more important. Encryption techniques play very important role in information security. In this project work, the performance of RSA algorithm is studied and analysed. Prime numbers are generated using various algorithms and verified their primility property. To meet current security requirement, iris recognition system is used to protect the keys from intruder. The performance of the iris recognition system is verified, where an automatic iris region segmentation method is presented using Daugman's operator. This iris region is normalized using Daugman's rubber sheet model, where the circular iris section is converted into rectangular block from which only 100 X 150 pixels are selected excluding eyelashes and eyelid part to avoid errors in the matching process. Finally, two unique prime numbers have been assigned to the selected rubber sheet model which acts as input to the modified RSA algorithm. For the matching of rubber sheet models PCA technique and Euclidean distance are used and their performance is verified. This method will be successful only if the iris image segmentation and matching is done properly. Otherwise, for a given data encryption and decryption processes will be failed. Segmentation is a main step in iris recognition, because the part which is wrongly identified as iris will corrupt the iris templet resulting in poor recognition. The algorithm is applied for 105 images of CASIA database and the precision for segmentation is approximately 85.71% i.e. 90 out of 105 images are segmented successfully.

REFERENCES

[1] William, Stallings. Cryptography and network security: principles and practices. Pearson Education India, 2006.
[2] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013)
[3] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." In Strategic Technology (IFOST), 2011 6th International Forum on, vol. 2, pp. 1118-1121. IEEE, 2011.
[4] Konigsberg, Zvi Retchkiman. "Primes and Twin Primes Generator Algorithms." In Computational Engineering in Systems Applications, IMACS Multiconference on, vol. 2, pp. 1-4. IEEE, 2006.
[5] Pittu, Ganesh Reddy. "Generating primes using partitions." arXiv preprint arXiv:1505.00253 (2015).
[6] Daugman, John G. "High confidence visual recognition of persons by a test of statistical independence." IEEE transactions on pattern analysis and machine intelligence 15, no. 11 (1993): 1148-1161.
[7] Masek, Libor. "Recognition of human iris patterns for biometric identification." (2003): 1-7.
[8] Wildes, Richard P. "Iris recognition: an emerging biometric technology." Proceedings of the IEEE 85, no. 9 (1997): 1348-1363.
[9] Krichen, Emine, M. Anouar Mellakh, Sonia Garcia-Salicetti, and Bernadette Dorizzi. "Iris identification using wavelet packets." In Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on, vol. 4, pp. 335-338. IEEE, 2004.
[10] Huang, Ya-Ping, Si-Wei Luo, and En-Yi Chen. "An efficient iris recognition system." In Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on, vol. 1, pp. 450-454. IEEE, 2002.
[11] Jong Gook Ko, Youn Hee Gil, Jang Hee Yoo, and Kyo Il Chung. "Method of iris recognition using cumulative-sum-based change point analysis and apparatus using the same." U.S. Patent 7,715,594, issued May 11, 2010.
[12] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." In Strategic Technology (IFOST), 2011 6th International Forum on, vol. 2, pp. 1118-1121. IEEE, 2011.
[13] Gries, David, and Jayadev Misra. "A linear sieve algorithm for finding prime numbers." Communications of the ACM 21, no. 12 (1978): 999-1003.
[14] Marc Joye, Pascal Paillier, and Serge Vaudenay. "Efficient Generation of Prime Numbers." In Cryptographic Hardware and Embedded Systems-CHES 2000: Second International Workshop Worcester, MA, USA, August 17-18, 2000 Proceedings, p. 340. Springer, 2003.
[15] Buddharpawar, Aniket S., and S. Subbaraman. "Iris Recognition based on PCA for Person Identification." International Journal of Computer Applications (0975–8887)(2015).
[16] Shi, Jin-Xin, and Xiao-Feng Gu. "The comparison of iris recognition using principal component analysis, independent component analysis and Gabor wavelets." In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 1, pp. 61-64. IEEE, 2010.
[17] Jagadeesh, N., and Chandrasekhar M. Patil. "Iris recognition system development using MATLAB." In Computing Methodologies and Communication (ICCMC), 2017 International Conference on, pp. 348-353. IEEE, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY