International Journal of Research in Advent Technology, Vol.4, No.7, July 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Implementation of Image Base Key Generation Method for Cryptography

Neminath J. Sanap[1], Dr. V. T. Gaikwad[2], Prof. H.N. Datir[3]
M.E (Pursuing) [1], Associate Professor[2], Assistant Professor[3]
Computer Science and Engineering[1], Information and Technology[2,3]
Sipna C .O. E. T, Amravati, Maharashtra, India
neminathsanap99@gmail.com[1], *vtgaikwad@rediff.com*[2], *h_datir@rediffmail.com*[3].

Abstract- In recent Era, there has been significant development in security technologies. Security in the real world is a most important issue to be taken care and to be encountered with different forward looking and preventive measures. Securing the information is the process of identifying and restricting the access of user's information from unauthorized access. Each and every level of information should stay away from all the security breaches. Privacy, Authentication is all what we all know and the way they work, but ultimately what we would like now is to work on network in the remote area to transfer the message. In this paper such as RGB images using proposed key generation method and we highlighted the technique called AES (Advanced encryption standard).Cryptography which has a potential capability to transform the secure information on the internet. Several existing algorithm for encrypting and decrypting the user messages are available everywhere the world, but generating the key for cryptography should be a difficult task to crack. The RGB image base key generation technique will work better than the traditional key generation method.

Index Terms- 16 byte key, AES decryption, AES encryption, Image and text cryptography, spilt RGB image, shuffle RGB image.

1. INTRODUCTION

Now a day's security is important issue in the information communication. The main objective of this study is to increase max security in communication by encrypting the information using a key that is created through using RGB image. Two way secure data communication most important recent time using cryptography. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately, thus, the concept of generating the key from an image came to the role [1]. Cryptography is considered to be one of the fundamental building blocks of provide information security. Cryptography presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination [2].

Cryptography is a powerful tool to achieve information security, the security of cryptosystems relies on the fact that cryptographic keys are secret and known only to the legitimate user [3].

In this paper, a new idea is suggested which is color image base key generation method different from any of the methods. In this new method, RGB image having three plane(R,G.B) generate 128 bit key which is shuffle image block 4*4 matrix Vertically up shift and Horizontally left shift increase step by step by matrix form and select R plane 8 byte or G plane 4 byte and B plane 4 byte to get 16 byte key.

The method uses a RGB image to generate a key which will be used in the encryption and decryption operations. Our method is distinguished from the other ones as the generated key length 16 byte varies according to the RGB image. The AES encryption and decryption algorithm more powerful other than algorithm and proposed algorithm is simple to implement and easy to use.

2. LITERATURE REVIEW

Santhi et al. [1], have proposed a novel algorithm for key generation using image features. This study uses the Gray Level Co-occurrence matrix of an image to extract the Gray Level Co-occurrence properties of the image. A 56-bit sub-key is generated from the extracted Gray Level Co-occurrence properties. Then the key for

encryption and decryption is generated using the sub-key generated from the image.

Seshadriand Trivedi [4], have proposed a method for generation of cryptographic key which is generated using biometrics. This can be efficiently solved by the integration of biometrics with cryptography. Conventional techniques depend on biometric features like face, fingerprint, hand geometry, iris, signature, keystroke, voice and the like for the extraction of key. Instead of storing key we will generate the key dynamically with the help of biometrics. Here we will use Finger print to generate key.

Wong et al. [5], have proposed a method for cryptographic key from webcam image. user's image from digital webcam shall be tested for its randomness according to the NIST Statistical Test Suite. Recommendation on using webcam images as source of random cryptographic keys.

P.Murali et al. [6], have proposed a method for true random number generator method based on image for key exchange algorithm. True random numbers based on image which generates 256 bits key or higher for key exchange algorithm. True random numbers are always secured and good, compared to pseudo random numbers.

Tanmay Bhattacharya [7], have proposed a method for a novel data encryption technique by genetic crossover of robust biometric key and session based password. The Biometric key generated from the fingerprint of the same user. The proposed approach trained the system by Artificial Neural Network in such a way that a small portion of the fingerprint is enough to generate the Biometric key which minimizes the chance of false rejection.

Farhan R. Patel [8], have proposed a method for performance evaluation of steganography and AES encryption based on different formats of the image present a combination of both these techniques wherein the text is first hidden into some form of cover image using Least significant bit (LSB) hiding method and then encryption using Advanced Encryption Standard (AES) is performed on to the stego image.

Saksham Wason et al [9], have proposed a method implemented security for text and image information using a cryptographic key. Based on the session type a key is generated which is used for encrypting and decrypting the messages which are transmitted between two sides. The length of the key varies in every session according to the session type.

Mohammed Tajuddin [10], have proposed a method for Cryptographic Key Generation using Retina Biometric Parameter. The key is directly generated from the human biometric information such as retinal blood vessels which is not stored in the database.

Priyanka et al, [11], have proposed a method Security in the real world is an important issue to be taken care and to be encountered with various proactive and preventive measures. Each and every level of information should stay away from all the security breaches. Privacy, Authentication how they work, but ultimately what its want now is to work on network in the remote area to transfer the message. The highlighted the technique called cryptography which has a potential capability to transform the secure information on the internet.

Tawfiq et al. [13] have proposed a method for encrypting the sender's messages using new algorithm with a secret key which is generated from using color image and the difference in the LSB of the image pixels. This key will be used for encrypting and decrypting the messages which are transmitted between two sides. The length of the key varies according to the size of the message as it varies in every session according to the session type.

3. ANALYSIS OF PROBLEM

One is that the color image size is almost always greater than that of text. Therefore, regularly cryptography need much time to encrypt the image data but in secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately, thus, the concept of generating the key from an color image came to the role.

4. PROPOSED WORK

The propose system is RGB image based key generation technique is a new approach to both the text and image (data) encryption, which aims to transfer confidential and authenticity transmitted them by cryptography algorithm information over a shared network. It includes the following steps as showed in figure.1.

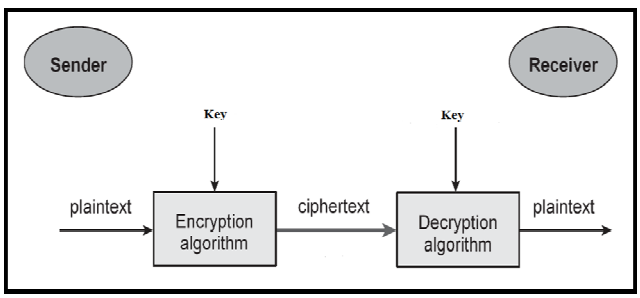

Fig. 1 Block diagram of Key Generation method sender side and receiver side

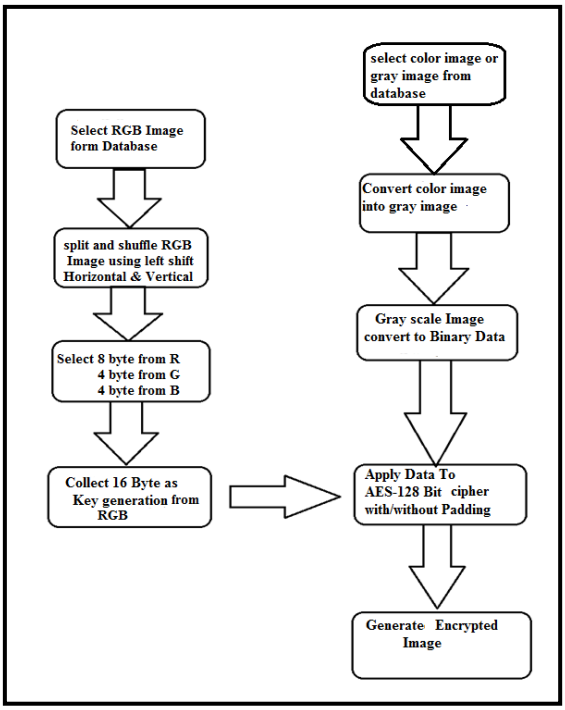

Fig. 2: Sender Side Block Diagram

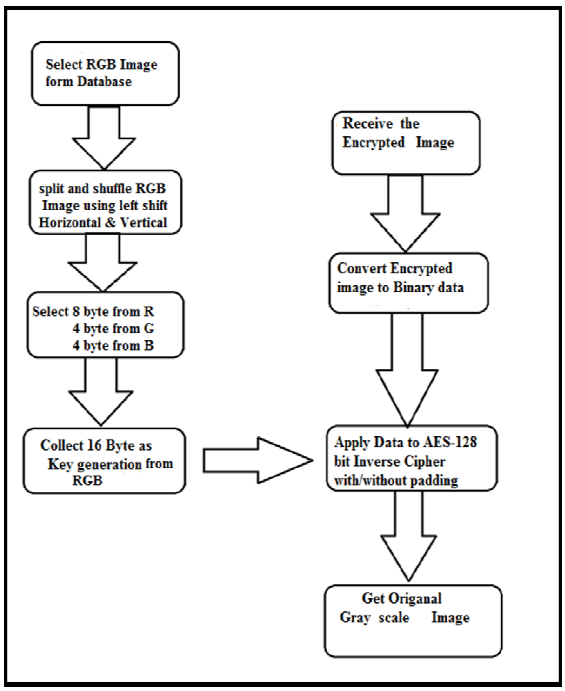

Fig. 3: Receiver Side Block Diagram

The Algorithm is divided up into four Levels which are given in Table 1.

Table 1: Level in the entire process

Level	Process
1	Database Creation
2	Key generation
3	Encryption
4	Decryption

4.1 Image Database:

In this level, consider a database of color RGB images which would be used for generating the key 16 byte for AES algorithm encryption/decryption process. In case of using the database should contain number of images, otherwise, both the sender and the receiver should use the same database of images as the names of the images should be the same in both sides.

4.2 Key Generation:

Key is generated from the color image stored in database based on the different type of image .In this level, RGB image used only authorized sender and receiver can access the image database. Color image is constructing of 3 images. Color digital images are made of pixels, and pixels are made of combination of primary colors, a plane is made of just one of these primary colors. In this paper we used one plane of RGB color image red, green or blue. So we have to shuffle image 4*4 block matrix vertically up shift and horizontally left shift increase step by step by matrix form and select R plane 8 byte or G plane 4 byte and B plane 4 byte to get 16 byte key. The method uses a RGB image to generate a key which will be used in the encryption and decryption operations

4.3 Encryption:

In this level, we present the AES-128 bit encryption algorithm the algorithm step as follows**.**
The AES standard states that the algorithm can only accept a block size of 128 bits. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption the

exception that each stage of a round its counterpart in the encryption algorithm. The four stages are as follows:

- Substitute bytes
- Shift rows
- Mix Columns
- Add Round Key

4.4 Decryption:

In this level, we present the AES-128 bit decryption algorithm the algorithm step as follows**.**
The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

- Inverse Shift rows
- Inverse Substitute bytes
- Inverse Add Round Key
- Inverse Mix Columns

5. EXPERIMENTAL RESULT

The results of AES algorithm based on data encryption and decryption for protection of data, along with results of AES algorithm, in this implemented work to check the strength of the approach system compare different algorithms technique, with the help of some output parameters namely the MSE value, PSNR value, the correlation value and the execution time. The Advanced encrypted standard (AES) algorithm is used in this work is evaluated and tested by applying the above parameters.
Now, this project emphasis on working of the proposed system and the GUI of MATLAB application consists of simple home screen, which contains some buttons for loading Data (text and image). In this project there are two different communication multimedia text and image along with data preview window, which show the data which have selected data.
It also shows the output of data encryption and decryption process performed in both input text and image, a text data given an input sender and image data selection of image from database.

The proposed key generation method having a choice for selection of RGB image to perform 16 byte generate image, Key is generated from the color image stored in database based on the different type of image. RGB image used only authorized sender and receiver can access the image database. Color image is constructing of 3 images. Color digital images are made of pixels, and pixels are made of combination of primary colors, a plane is made of just one of these primary colors.

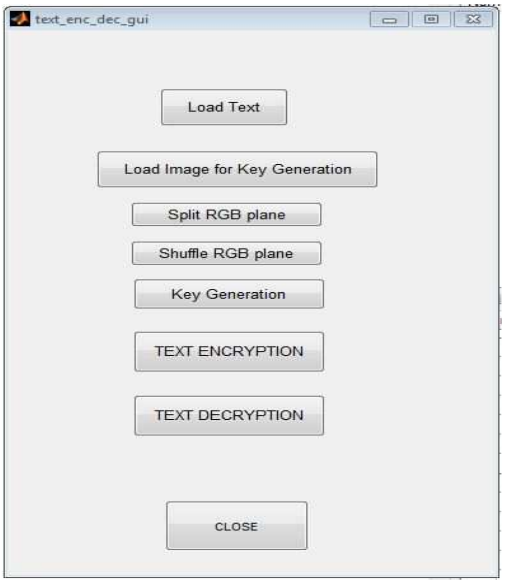

Fig. 4: Main Text Encryption and Decryption GUI Window

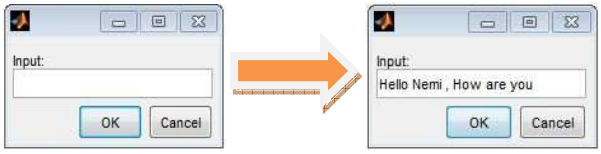

Fig. 5: Input Text GUI Window

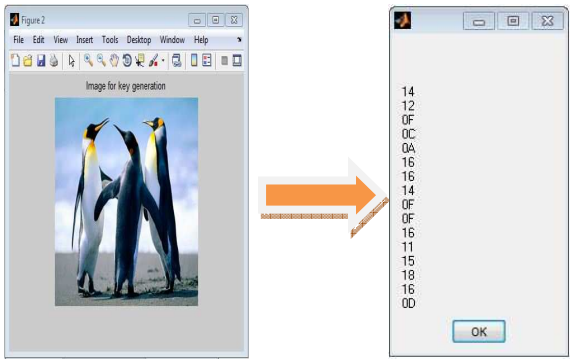

Fig. 6 : Showing the image for 16 bit key generation.

On this text GUI, second click on ‘Load image for key generation’ button. This will correspondingly result into launching of a new window named ‘Pick a color image for key generation’. Here users have to select color image for key generation. The user simply need to select appropriate color image in the window and click on ‘open’ button, which will load the color image and display a small scaled preview of the loaded color image.

The text GUI, third click on ‘spilt RGB plane’ button, a color image combination of three planes, The Fifth click on ‘Key Generation’ button, a color image generate key collect image pixel select R plane 8 byte

or G plane 4 byte and B plane 4 byte to get 16 byte key.

Fig. 6: Input text encryption and decryption display.

The sixth click on 'Encryption' button, to apply 128 bit AES algorithm text encryption step as add round key, shift row, sub bytes and mix columns. Then seven click on 'Decryption' button, to apply decryption AES algorithm step as inv add round key, inv shift row, inv sub bytes and inv mix columns.

The proposed system is having a select data (gray or color image) for cryptography method to perform image encryption and decryption; the choice can be made by means of selecting the buttons named by the image encryption method and image decryption method. Each perform corresponding cryptography method on both input images sender original and receiver encrypted image Along with original image output, system also provide MSE and PSNR as the output parameter for both encryption and decryption methods. This will be also very helpful for output evaluation and comparison of implemented image cryptography technique. Along with this to achieve good discrimination and security also apply some operations like sending data. Finally with help of all these factors the result is concluded.

Results showing the performance parameters for combination of cryptography observing the results in table 2, and evaluating the performance based upon only cryptography it learn that image is the best format which supports cryptography, also the criteria of zero value MSE and infinity value PSNR both value indicate that give original image output both are together satisfied by the image.
The image encryption fig.7, in GUI click on 'Encryption' button, to apply 128 bit AES algorithm image encryption step as add round key, shift row, sub bytes and mix columns. The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption the exception that each stage of a round counterpart in the encryption algorithm.GUI, click on 'Key Generation' button.

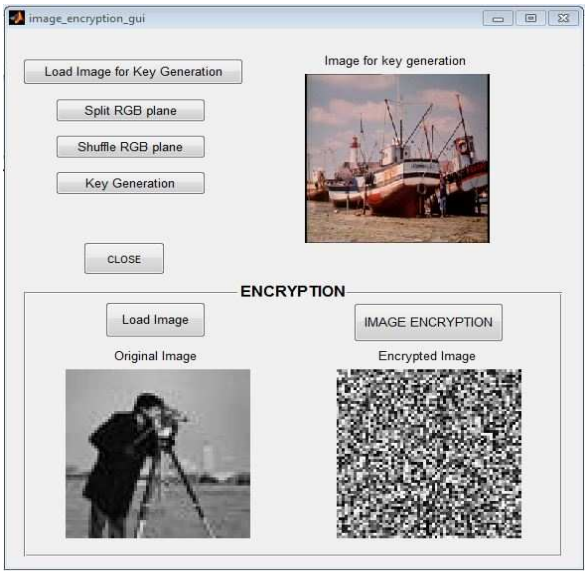

Fig. 7: Implementation of AES encryption on cryptography image

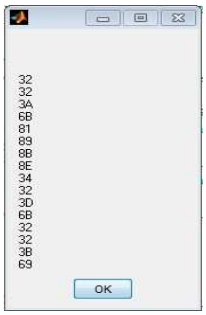

Fig. 8: The RGB image generate 16 byte key

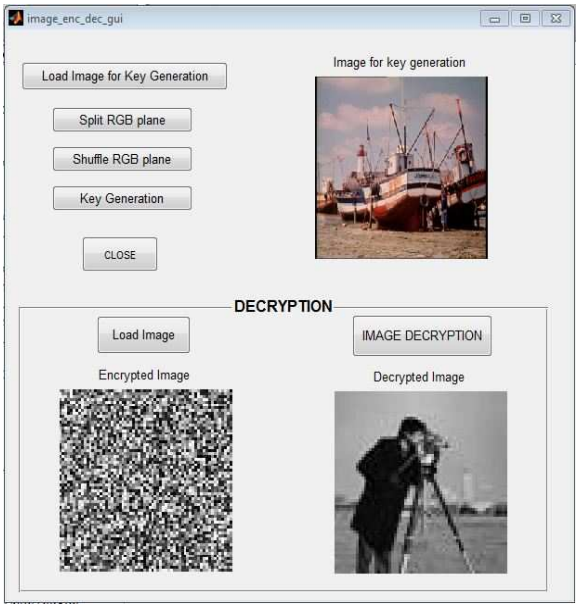

Image Dataset	PSNR Value	MSE Value	Corre-lation Value	Execution Time Sec
Lena	Inf	0	1	42
Pepper	Inf	0	1	44
Baboon	Inf	0	1	45
Airplane	Inf	0	1	46
Barbara	Inf	0	1	48
Camera man	Inf	0	1	44

Table 2: Results showing the performance parameters for AES algorithm

A color image generate key collect image pixel select R plane 8 byte or G plane 4 byte and B plane 4 byte to get 16 byte key. As a result to this, fig.8 the method uses a RGB image to generate a key which will be used in the encryption and decryption operations.
The image enc dec GUI, click on 'Decryption' button, to apply decryption AES algorithm step as inv add round key, inv shift row, inv sub bytes and inv mix columns, As a result to this, fig.9 show encryption and decryption data.

6. CONCLUSION

The Cryptography provides more security to the data which is transferred in publicly shared multimedia. When the cryptography keys are long and complex, it will be can't identify by the attacker, but it will be difficult to remember. The security of the cryptographic system relies on the fact that the cryptographic keys are secret and known only to the legitimate user. Thus new Cryptography approach shows the key generate and the encryption for different Messages.
A method base on the key that is generation directly from an image stored in the database and the process of key Generation base on shift row left and column shift upward This creates more complexity to crack or guess the cryptanalysis techniques. To break this algorithm, it is need to know the images database, color image plane. This process is more secure that any RGB image can be used for key generation as the key generation is directly based on the image RGB plane content.

Fig. 9: Implementation of AES encryption on cryptography image

7. ACKNOWLEDGEMENT

It is a matter of great pleasure by getting the opportunity of highlighting fraction knowledge, I acquired during my technical education through this paper. This would not have been possible without the guidance and help of many people. This is the only page where I have opportunity of expressing my emotions and gratitude from the care of my heart to them. This paper would not have been successful without enlightened ideas; timely suggestion and keen interest of my respected Guide **Dr. V. T. Gaikwad** without his best guidance this would have been an impossible task to complete.

8. FUTURE SCOPE

Implementation of Cryptography using AES algorithm together were performed with text and images, but this method can be further be extended to audio, video as well thereby include the security in the audio and video processing.

REFERENCES

[1] Santhi, B., K.S. Ravichandran , A.P. Arun and L. Chakkarapani, "A Novel Cryptographic Key Generation Method Using Image Features" ,Research journal of Information Technology 4(2):88-92,2012.
[2] Cryptography and Network Security- Principle and practice, "William Stalling" ,Pearson Education third edition.
[3] Asha Ali, Liyamol Aliyar and Nisha V.K, "RC5 Encryption Using Key Derived from fingerprint Image" Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International conference,28-29 Dec 2010.
[4] Seshadri,R.and T.RanhuTrividi, "Efficient Cryptographic Key Generation using Biometrics" ,Int .J.Comp.Tech.Appl., Vol 2(1),183-187.
[5] Wongsiaw Lang , NurAzman Abu ,Shahrin Sahib, "Cryptography key from Webcam Image for Key Exchange algorithm ", 2009 International Symposium on Computing ,Communication , and Control.

[6] Murli ,P. I and R.Palraj , "true random number generation method based on image for key exchange algorithm",2009 International Symposium on Computing Communication ,and Control.
[7] Tanmay Bhattacharya ,SirshenduHore, Ayan Mukherjee and S.r.BhadraChaudhuri , "password A novel data encryption technique by genetic crossover of robust biometric key and session based" .International Journal of Network Security & Its Application (IJNSA), Vol.3, NO2,March2011.
[8] Farhan R. Patel, Dr. A. N. Cheeran. "Performance Evaluation of Steganography and AES encryption based on different formats of the Image" International Journal of Advanced Research in Computer and Communication Engineering. Vol. 4, Issue 5, May 2015.
[9] Saksham Wason,Piyush Kumar,Shubham Rathi, "Text and image encryption using color image as a key" Internatonal Journal Of Innovative Research In Technology 2014 IJIRT | Volume 1 Issue 5 | ISSN: 2349-6002.
[10] Mohammed Tajuddin, C. Nandini , " Cryptographic Key Generation using Retina Biometric Parameter" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013.
[11] Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K, " A New Randomized Cryptographic Key Generation Using Image" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013.
[12] Advanced encryption standard (aes) Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology, November 26, 2001.
[13] Tawfiq S. Barhoom, Zakaria M. Abusilmiyeh, "A Novel Cryptography Method Based on Image for Key Generation" , 2013 IEEE 2013 Palestinian International Conference on Information and Communication Technology,10 Nov. 2013.