ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

i-S^{2}SLE: An Encryption methodology for Securing Image using Linear Algebraic Equation

N.Kanagaraj
Research Scholar
Department of Computer Science and Engineering
Alagappa University Karaikudi, TN,India
kanagaraj.n.in@ieee.org

Dr. A. Padmapriya
Associate Professor
Department of Computer Science and Engineering
Alagappa University Karaikudi, TN, India
mailtopadhu@yahoo.co.in

***Abstract*— In today's online world, there isa huge amount of cryptographic and steganographic techniques which are used to transfer the data safe and secure between sender and receiver. In this paper, an encryption methodology (i-S^{2}SLE) is presented to secure the image using linear equation based on shuffling and substitution processes. First, the original image is shuffled in two different ways and then the resultant image is encrypted using a key, which is determined using a linear equation. The resultant image is encrypted well enough to be sent on a public network. On the receiver side, the reverse process is done in order to get back the original image. The work is implemented using JAVA. The experimental results show that the proposed system can maintain its secrecy even in the worst situation.**

Keywords— Cryptography, Linear algebra, Image, image encryption, decryption.

I. INTRODUCTION

Internet has the wide variety of applications like online purchasing, bank transactions, communications and so on. In communication, the image needs to maintain its secrecy or confidentiality. The intruder can break or open up the data and can read/alter the data. On the internet, nobody knows how the data being sent. Still, everyone needs their data to be sent in a secured way; in some way.

Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to encrypt or hide their existence [2]. These techniques have been used in the online communication; particularly for protecting e-mail messages, credit card information, corporate data, etc.

More specifically, cryptography [8] is the study of mathematical techniques related to attributes of information security such as data integrity, confidentiality, authentication and non-repudiation.

Cryptography maintains the secrecy by changing the original image to disguised format. It is useful to achieve confidential transmission over a publicly available network. The original image is converted to a cipher image by using a key. Only those who possess a secret key can decode the cipher image to plain image. Cryptanalysis is an analysis on the plain image or cipher image to decode without the original key.

There are two different techniques in securing images; differentiated by the key usage. They are, i) Symmetric key, and ii) Asymmetric key encryption. The proposed algorithm works on symmetric key technique.

The aim of this paper is to introduce a new methodology of encryption technique for better security to the image, through image processing. In particular, an encryption system is presented in this paper, which uses shuffling [4-6] and substitution processes using a linear algebraic equation. It can able to perform on almost any kind and size up to 1024*1024, with an ease of way. The ideology of this paper is inspired from the paper [1]. S^{2}SLE is an encryption methodology used to encrypt the text using shuffling and substitution techniques. The paper divided into three sections. In the first section, the proposed methodology is explained. In the second section, the work flow of the proposed methodology is elaborated briefly. The third section describes about the experimental study. In the final section, the conclusion is discussed.

II. PROPOSED METHODOLOGY

In this proposed methodology, the image's RGB values are shuffled. Shuffling process has two steps of processes. In the first step of shuffling, the R-G-B values are interchanged. In the second phase of shuffling, the values of 'R' are shuffled in odd or even order. These two steps of processes make the look of the resultant image as different one.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

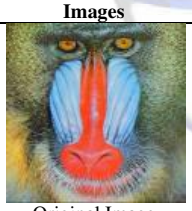
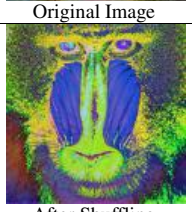
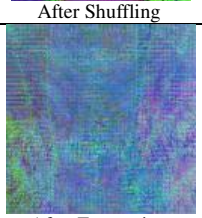
Fig. 1. represents the image after the shuffling process.

Shuffling cannot make a drastic change in the original image. Table1and figure 1 are used to assess the above statement. If the two images are same, the Peak Signal-to-Noise Ratio (PSNR) will be infinity. If the PSNR [7] value is less, then it reveals that the image is exposed very less during external attacks.

The encryption is neededfor better security for the image, the resulting image is encrypted using a key (with the help of an Exclusive-OR operator), which is created from a linear algebraic equation.

A set of linear equation is used for choosing one linear equation in a random fashion. A set(S) can hold 'n' number of linear equations. The total number of linear equations (n) decides the security level in *i*-S^{2}SLE system. According to the key, the number of rounds in the encryption process is decided. The number of rounds is helpful in the better security process. The detailed explanation of the proposed methodology is done in the next section for better understanding.

TABLE 1 REPRESENTS THE PSNR VALUE BETWEEN THE ORIGINAL IMAGE AND THE RESULTANT IMAGES.

Images	PSNR Values
 Original Image	Infinity
 After Shuffling	19.04
 After Encryption	19.90

III. WORK FLOW

i-S^{2}SLE system has four steps of processes. They are i) Key generation, ii & iii) Shuffling processes, and iv) Substitution. In the first phase, a linear algebraic equation is chosen from the set(S). The linear algebraic equation is solved using a random number. The solution taken as a key (K) for the encryption purpose and it is also used in the shuffling process (Third phase). Figure 2 represents this stage. The 'K' value converted into bits and the digits are summed up. If the final value is '0', it represents odd order shuffling and if the final value is '1', then it represents even order shuffling.

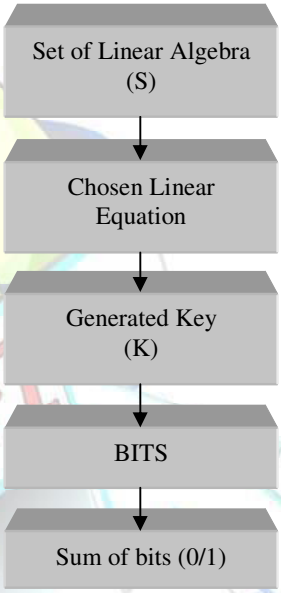


Fig. 2. represents the process of generation of key.

The next two phases relate to the shuffling process. The proposed encryption system can take an image with size up to 1024*1024. The R, G and B values are taken in a separate one-dimensional array (for each band). R, G and B are interchanged and this is the second process of encryption system. In the third phase, the values in the array are re-arranged in odd or even order. The resultant image (RSi) holds the shuffled value, but not encrypted.

In the last phase, the image (RSi) is encrypted using the 'K' value with an Ex-OR operator. The rounds of encryption process are decided using the 'K' value. The resultant image will be encrypted in a good manner.

IV. EXPERIMENTAL STUDY

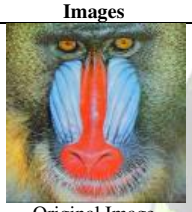
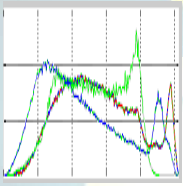
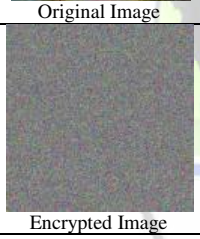
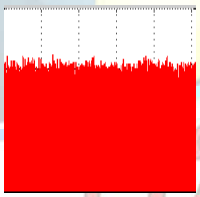
The experimental study is done on *i*-S^{2}SLE using a personal computer equipped with an Intel processor (Core

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

i3) with a clock speed of 1.7GHz, 2 GB of RAM and 520 GB of Hard disk capacity. The PSNR and histogram [3] values are taken into account to assess the strength of the *i*-S^2SLE algorithm. In the proposed methodology section itself the PSNR values between the original image and its resultant images are discussed briefly.

The histogram is the graphical representation of the dispersion of R, G and B values. If the histogram shows the band values dispersion in equal or average, then the encrypted image cannot be broken using statistical attacks. Different set of images has been used to justify the strength of the proposed algorithm. From the table 2, it is possible to assess the *i*-S^2SLE; that the encrypted images won't reveal any data during attacks.

TABLE 2 REPRESENTS THE HISTOGRAM DIFFERENCE BETWEEN THE ORIGINAL IMAGE AND THE ENCRYPTED IMAGE.

Images	Histogram
 Original Image	
 Encrypted Image	

V. CONCLUSION

This paper describes about an image encryption technique using the concept of linear equation. The linear equation is sensitive to the random values. The proposed method utilizes the randomness of the linear equation in order to encrypt the image. In this algorithm the pixel position is shuffled in an order according to the key value, which is derived by linear equation. The experimental study clearly states that this algorithm completely removes the similarity of the encrypted images to the original images, the distribution characteristics of RGB-level matrices. This methodology can be improvised by using the Linear Diophantine equation or a chaotic map instead of using alinear algebraic equation.

REFERENCES

[1] N. Kanagaraj and Dr. A. Padmapriya. "S^2SLE: An Encryption Methodology for Securing Data using Linear Algebraic Equations". Journal of Computer Science and Applications Vol. 6, No.1, pp.no.309-312. ISSN 2231-1270.

[2] Bloisi, D., Iocchi, L., "Image based Steganography and Cryptography", International Conf. on Computer Vision Theory and Applications (VISAPP), 2007.

[3] Rafael C.Gonzalez, Richard E. Woods, "Digital Image Processsing (2nd ed.), Pearson Education, ISBN 978-8178086293.

[4] Reji Mathews, Amnesh Goel, PrachurSaxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6

[5] Amnesh Goel,Nidhi Chandra, "A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", IJIGSP, vol.4, No.2, pp.16-22, 2012.

[6] Quist-Aphetsi Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling", International Journal of Computer Network and Information Security, 7, pp. 43-50, 2013. DOI: 10.5815/ijcnis.2013.07.05

[7] "Peak Signal-to-Noise Ratio as an Image Quality Metric": White paper published by National Instruments China (2013)

[8] William Stalling, (March 2013), "Cryptography and Network Security: Principles and Practice" (6 ed.), Prentice Hall, ISBN 978-0133354690.