Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL

Reji Mathews *Member IAENG*, Amnesh Goel *Member IAENG*, Prachur Saxena, Ved Prakash Mishra

***Abstract* - The image encryption has become the most important focus point in this era of breach of security and confidential information contained within a piece of data. Hence proposing a new method of encryption methodology in which the focus is on complete breakdown of image into its RGB components and then performing the shifting and permutations on these elements based on a key. The inter-pixel shifting of R G B values changes the shade of the entire encrypted image so as to contain minimum clues for guessing out the light and shade profiles of the original plain image. An element of secrecy in the basic algorithm is also introduced in the method.**

***Index Terms* - inter pixel, image encryption, RGB, shifting.**

I. INTRODUCTION

There has been an increasing breach in the confidentiality of certain sensitive data due to large number of attackers evolving day by day focusing on exploiting secret information meant for some purpose or some specific users. Today large number of transfer of data and information take place through internet, which is considered to be most efficient though it's definitely a public access medium. Hence to counterpart this vulnerability, many researchers have come up with efficient algorithms to encrypt this information from plain text into ciphers. The chaotic confusion and pixel diffusion [1] methods proposed by Friedrich perform the permutations using a chaotic 2-D [2] combined with alterations of Grey-Level values of each pixel in a sequential manner. Repeated rounds of permutations and alterations where used to achieve higher security and resistance to attacks. It was experimentally verified that the amount of time overhead in performing complex calculations and the complex diffusion process had led to large time complexity of the system.

Manuscript received March 06, 2011; Revised April 01, 2011.
This work was supported financially and sponsored in part by the ASET, Computer Science & Engineering department of Amity University, U.P, India.
Reji Mathews is with the ASET, Amity University, Sector 125, Noida, U.P, India pursuing Masters in Computer Science & Engineering (M.Tech). IAENG Member number: 111979. Phone number: 0091 9971956608; fax: 0091 469 2651856; e-mail:contactreji@gmail.com.
Amnesh Goel is with the ASET, Amity University, Sector 125, Noida, U.P, India pursuing Masters in Computer Science & Engineering (M.Tech). Phone number: 0091 9899953238; e-mail: amneshgoel7@gmail.com.
Prachur Saxena is with the ASET, Amity University, Sector 125, Noida, U.P, India pursuing Masters in Computer Science & Engineering (M.Tech). Phone number: 0091 9899604822; e-mail: prachur.saxena@gmail.com
Ved Prakash Mishra has provided guidance in completion of this research. He has completed his masters in Computer Science & Engineering (M.Tech) and now with Amity University, Noida, U.P, India as lecturer. Phone number: 0091 9958705144. Email: mishra.ved@gmail.com.

Many highly effective and secure algorithms like RSA[3], DES [4] and so on where used efficiently to encrypt the textual data. But in the domain of the Image Encryption, these algorithms proved to be less effective or rather impractical due to the characteristic features of images like the high byte size of the data to be encrypted and the complex structure of the image data. In permutations [5] and diffusions, the algorithms are designed to spread the change to a single pixel to larger area of the image. Such process can be very slow when it comes to voluminous data to be encrypted at competing speeds.

The initial methods of encryption the image using the pixel shifting and altering of the grey levels provided a large key space. The pixel shifting was performed by the non linear chaotic algorithm [6][7]. Though this method didn't change the shading or color profile of the pixel considerably so as to fully withstand the clever attacking algorithms. For e.g., a good attacker can at least guess from the color profile of the shifted image if the same was shot in bright sunny day light or if it was clicked indoors in a dark room.

The encryption on the image plane can be easier and less complex than working the same on the bit level. This involves scattering or distribution of the pixels element values over image plane. Another technique of the same kind is to avoid modification of any present bit values and instead shift the R G and B values between the pixels on the image plane. The Shifting can be governed by the help of a secured key value. The sequence of vertical and horizontal shifts can also be used as sensitive information of the technique being used to get the image encrypted.

A new method on spectral fusion of information has been proposed for optical encrypted color images in which images are decomposed into 3 basic color components [8]. Pertinent information fusion is considered as segmentation Encryption [9] consists of modulating each of color components by corresponding phase mask, which includes pertinent information collected from encrypted color keys according to various fusion criterions [10].

II. PROPOSED METHOD

In the proposed method, there are no alterations performed on the bit values. Instead the numerical values are shifted away from its respective positions. The total change in the sum of all values in the image (Δsize= SumofValuesRBG_plaintext – SumOfValuesRGB_cipher =0). Hence it is obvious that there

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

is no change in the total size of the image during encryption and decryption process. The attribute *size of image* will remain unaltered while the encryption process is being performed.

The image is looked at as a decomposed version in which the three principle component which forms the image is chosen to act upon by the algorithm. The R-G-B components can be considered as the triplet that forms the characteristics of a pixel. The pixel is the smallest element of an image which can be isolated and still contains the characteristic found in the image.

The RGB values are shifted out of its native pixel and shifted into some other pixel in lying within the image boundaries. The shift performed is linear and circular. The circular shift ensures that there is no loss of data or overwriting of the values. The Shifting of the values are governed by certain rules and inferences from the key provided at the beginning of the process.

The encryption process takes into consideration following values for the entire conversion of the plain image into the cipher image ready for transmission through the 'vulnerable' medium of transmission and definitely vice versa.

$\alpha_r[]$, $\alpha_g[]$, $\alpha_b[]$: The Shift displacement of the R G and B values known termed as the component displacement factor array which is different for R, G and B. This ensures that in each successive row, the displacement of a component doesn't remain a constant. Else it will result in the simple circular shift of the entire component and hence it becomes a favorable condition for the cryptanalyst.

PM []: Shift pattern mask array which is a string consisting of 1's and 0's. The size of the array is the total number of vertical and horizontal shifts performed in the course of the encryption process. Each 1 represents a circular vertical shift and a 0 initiates a circular horizontal shift. The PM[ ] can be derived from the secret key or else it can be supplied separately. This can form the subset of the keys. As the length of the mask increases, the security efficiency and time for encryption process increases.

III. ALGORITHM

The algorithm for the encryption process takes into account the image boundary limits viz. x axis and y axis coordinate limits. Since the algorithm works on the principle of circular shifting of the values, these limits have to be precise.

The same set of actions are performed on all the three components of the pixel namely R, G and B values. Whenever we take into consideration each component of the pixel, the amount of circular shift performed at eachiteration of the outer loop is different from the previous one. This technique avoids the effect of simple shifting of the entire image as a whole but helps in scattering off the color definition. Hence the importance of the inputs $\alpha_r[]$, $\alpha_g[]$, $\alpha_b[]$ comes into prevalence.

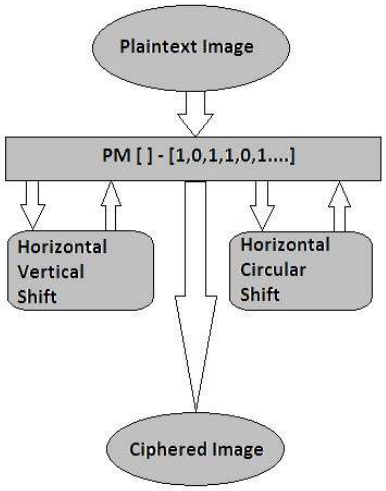


Fig .1.The proposed inter-pixel shift encryption scheme

The entire process is subdivided into 3 main modules given below. The control starts form the Perform_Encryption() method which calls the two sub modules VERTICAL_Shift() and HORIZONTAL_Shift() with respective relevant parameters.

Perform_Encryption( ) Method:

1:An Input Image with x coordinates x_0 to x_{max}
2:Y coordinates y_0 to y_{max}
3:PM[ ]
  3.1: Initialize Counter=1, initJump= Any Arbitrary Integer
  3.2: Loop while PM[counter] is not NULL
    3.2.1:if PM[counter]=1
      Invoke HORIZONTAL_Shift(x_{max},y_{max}, α_r[counter], α_g[counter], α_b[counter])
      Increment counter by 1.
      Endif
    3.2.2:if PM[counter] = 0
      Invoke VERTICAL_Shift(x_{max},y_{max}, α_r[counter], α_g[counter], α_b[counter])
      Increment counter by 1.
      Endif
    Endloop
4: Terminate

The two methods invoked the main encryption pseudo code are used to perform the vertical shift and horizontal shift of the pixel components.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The VERTICAL_Shiftmethod takes the x coordinates limits, y coordinate limits along with the component displacement factors from the main encryption pseudo code.

The VERTICAL_Shift method is defined in the following steps:

VERTICAL_Shift ( ) method:

1: Input image with its coordinate limits x_0 to $x_{max}y_0$ to y_{max}.
2: α_r[counter], α_g[counter], α_b[counter]
3: ΔR= initJump + α_r[counter]
4: ΔG= initJump+ α_g[counter]
5: ΔB= initJump + α_b[counter]
6: Loop and Repeat steps for ColC = x_0 to ColC= x_{max}
Do Circular Vertical Shift of R values at ColCth column by ΔR pixels
Do Circular Vertical Shift of G values at ColCth column by ΔG pixels
Do Circular Vertical Shift of B values at ColCth column by ΔB pixels
$\Delta R = \Delta R + \alpha_r$[counter]
$\Delta G = \Delta G + \alpha_g$[counter]
$\Delta B = \Delta B + \alpha_b$[counter]
Endloop
7: Return

The HORIZONTAL_Shiftmethod takes the x coordinates limits, y coordinate limits along with the component displacement factors from the main encryption pseudo code.

The HORIZONTAL_Shift method is defined in the following steps:

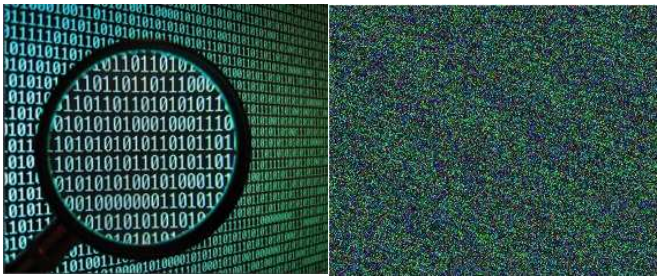
HORIZONTAL_Shift ( ) method:

1: Input image with its coordinate limits x_0 to $x_{max}y_0$ to y_{max}.
2: α_r[counter], α_g[counter], α_b[counter]
3: ΔR= initJump + α_r[counter]
4: ΔG= initJump+ α_g[counter]
5: ΔB= initJump + α_b[counter]
6: Loop and Repeat steps for RowC = y_0 to RowC= y_{max}
Do Circular Horizontal Shift of R values at RowCth row by ΔR pixels
Do Circular Horizontal Shift of G values at RowCth row by ΔG pixels
Do Circular Horizontal Shift of B values atRowCth row by ΔB pixels
$\Delta R = \Delta R + \alpha_r$[counter]
$\Delta G = \Delta G + \alpha_g$[counter]
$\Delta B = \Delta B + \alpha_b$[counter]
Endloop
7: Return

IV. SIMULATION RESULTS

The simulation was performed on the Matlab application to check the effectiveness of the algorithm. The initial test where conducted with the values selected for R G B displacement factors as 12, 24 and 36 respectively. The PM[ ] mask was fed with the values [1,0,1,1,0,1]. Theset of component displacement factor was selected as 12, 14 and 15 for red, blue and green respectively. For better security requirement, the length of the shift pattern mask was increased and more randomized combination of 1's and 0's where carefully selected.

The output of the algorithm with the above picked subset of key values is shown below.



(a) (b)

Fig (2): (a) shows plain image (b) Shows encrypted cipher image.

V. SECURITY ANALYSIS

The success of an effective encryption method is its resistance to various cryptanalytic attacks such as brute force attack and statistical attack. The efficiency in terms of brute force attack can be justified since the variable length of the shift pattern mask is a good confusion for the cryptanalyst. The subset of the keys consist of the different shift displacement factors for R G B values, the initial displacement for each of them before the key is applied and the shift pattern mask. Hence the key space analysis shows a large range of available keys which is quite resistant to brute force attacks.

The most favorable condition for a statistical cryptanalyst is the correlation between the adjacent pixels. As mentioned in [2], each pixel is highly correlated with the adjacent pixel in a normal plain image.

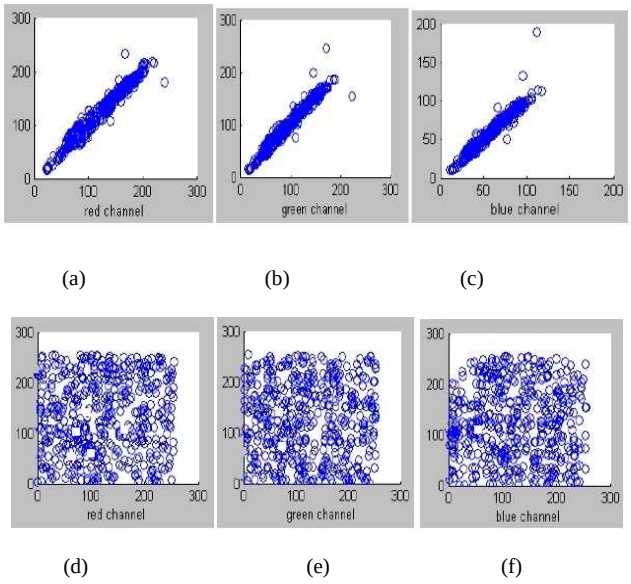
The correlation analysis was performed between the two diagonally adjacent, vertically adjacent and horizontally adjacent pixels in the ciphered image. Ideally ciphered image should have no correlation in the adjacent pixels.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Fig 3 shows the distribution of 2 horizontally, vertically and diagonally adjacent pixels. The following formula was used to compare the vertical and horizontal correlations of the adjacent pixels in the plain and ciphered image.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))^2,$$
$$\mathrm{conv}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)(y_i - E(y_i)),$$
$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where the value of 2 adjacent pixels was denoted with x_i and y_i and N is the number of pixels selected from the image in total.



(a) (b) (c)

(d) (e) (f)

Fig (3) : (a) Correlation analysis graph of Red channel Horizontally (b) Green Channel Vertically (c) Blue Channel in the plain image diagonally. Frame (d), (e) and (f) shows the analysis in ciphered image

VI. PROSPECTS OF THE PROPOSED METHOD

The main advantage of this concept is the high success of the algorithm in batch processing. A set of 'n' number of images can be tiled together to simulate as a single image and it can be processed with the proposed algorithm. In post encryption stage, the single image can be sliced back into the dimension of the original text images and rearranged before transmission over a public medium.

The same technique can be implemented by forming an image arranging one or more key images adjacent to the original plain image and executing the algorithm.

The encryption method was proven to be very strong in combination with the weaker and less secure encryption techniques for which the crypt analysis had already been performed. The combination of the weak technique with the above mentioned algorithm proved to be highly resistant to various attacks.

VII. CONCLUSION

The encryption algorithm to perform the conversion of plain image to cipher image has been successfully tested through simulations in MATLAB. The cipher image generated has been checked for the possible vulnerabilities towards an attack and the algorithm has proven to be effective against all the known crypt analytical strategies.

VIII. FUTURE WORKS

The successful implementations of the above algorithm have revealed a huge potential in the encryption algorithms involving the shifting of the three basic components of a pixel. This technique can be applied in various patterns. The future work considers a new strategy in which the Recursion Algorithms will be employed to perform the shifting. The slicing and rearrangement of the image parts at each iteration of a loop with respect to a secret key can make the ciphering technique extremely resistant to evolving cryptanalytic techniques. The research on the recursive technique is under process.

REFERENCES

[1] M. Salleh, S Ibrahim and I.F. Isnin, Image encryption algorithm based on chaotic mapping.JurnalTeknologi, 39(D) Dis. 2003: 1–12 UniversitiTeknologi Malaysia.
[2] R.Kadir, R.Shahri and M.A.Maarof, A modified image encryption scheme based on 2D chaotic map. 978-1-4244-6235-3/10/2010 IEEE.
[3] RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-2-6.html
[4] DES. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. The url explains the concept of the Data Encryption Standard.
[5] S.Xu, Y.Wang, J.Wang and U.Guo. A fast encryption scheme based on a nonliner chaotic map.2010 2nd International Conference on Signal Processing Systems (ICSPS).978-1-4244-6893-5/2010 IEEE.
[6] Sobhy, M. I. and A. R Shehata. 2001. "Chaotic Algorithms for Data Encryption". IEEE, 0-7803-7041-4.
[7] Z.Minguming and T.Xiaojn, A multiple chaotic encryption scheme for image. 978-1-4244-3709-2/10/2010 IEEE.
[8] J.Fan and Y.Zhang, Color image encryption and decryption based on double random phase encoding technique. 978-1-4244-4412-0/09/2009 IEEE
[9] R.E. Sawda, A.A.Falou, Gilles Keryer and A.Assoum, Image encryption and decryption by means of an optical phase mask. 0-7803-9521-2/2006 IEEE.
[10] Rami El Sawda, AymanAlfalou, HabibHamam, "RGB Colored Image Encryption Processes Using Several Colored Keys Images," fgcn, vol. 2, pp.594-598, Future Generation Communication and Networking (FGCN 2007) - Volume 1, 2007.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)