Image Encryption based on Random Point Image Slicing and Recursive Application of RGB Value Displacement on Slices

Amnesh Goel
Amity School Of Engineering
& Technology, Amity University,
Noida (U.P.), India

Nidhi Chandra
Amity School Of Engineering
& Technology, Amity University,
Noida (U.P.), India

ABSTRACT
The image encryption methods have become very important in the today's scenario because images are widely used for various purposes and transmission of digital image over network has increased drastically. Handling of images demand more security as they contain confidential information in it and the concept of encryption has been used for years. Here we proposing a new enhancement to the algorithm of image encryption proposed earlier where the image slicing is perform followed by shuffling up those slices. In this research compilation, we derive the point or coordinate from the key value on basis of which we bifurcate the image into 4 parts and the Inter-pixel displacement of RGB attributes are applied to each of this part. Similarly this process is continued with a new point coordinates till the predefined number of iterations are donewhose count is again a value derived from the encryption key.

Keywords
Image Encryption, RGB, Shifting, Slicing, Shuffling, Permutation, Random Point.

1. INTRODUCTION
The image encryption methods are widely used now a day in various fields to store confidential information from defence services to medical services and personal use to official use. Use of images has increased drastically in last two decades since when cost of camera is decreasing up to an affordable level of common man; and when its efficiency is increasing in terms of its quality. Although prior to that image were only limited to personal use like clicking pictures on some event i.e. birthday party, marriage etc. and were a part of the film industry. Since from 1990, when colour models were introduced to enhance quality of image, the hidden potential of images came into picture and its usage increased in various domains.

Images are extensively used to store the biological information which is unique of every human being and unauthorized access to that information can lead to waning privacy. Indian government has launched one project with name AADHAR [1] which consist of biological scan of body for every Indian person. Even, now a day, most of the security systems are including biological scan to authenticate the individual persons. Images for this purpose could be either finger scan or hand scan or scan of any other part of the body which is taken for authorization. In this way the use of image requires storages in such a way that no one could first easily access it and second even if someone gets the images even then no one should get information from it. So a perfect encryption mechanism is requiring achieving this.

Images are broadly using in this era for archival purposes to store historical government records in image format after scanning them because keeping them in paper format only can lead to problem as those papers are stick in hard files for so many decades and referring them and keeping them safe from disasters like fire is big problem in itself, and unofficial access to those papers also easy. So, government is planning to move towards digital medium to store them permanently which is safest move at this time.Hence, keeping this in mind, government is launching soon a project which will convert all historical documents into the image format of any format, so that the hassle of safety can be keep aside but in this another problem arises and i.e. of security of images as now that information will be in digital form and hackers will definitely try to get that information. So, better image encryption methods are required.

Image encryption methods gain popularity too because of its use over the public open network where anyone can access data without much effort. As the technology advancing at very high speed, human dependency on internet has increased in the same frequency in both the fields' i.e. personal use and in commercial use. Flow of images over internet has increased and much this flow of images over network is now part of many applications. To complete the application process, it is necessary to flow images over network like in banking domain, now finger scan enable ATM machines [2] [3] are in use where a bank account holder need to give finger scan input to complete the transaction and in backend this finger scan goes over network to check the authentication of user; and this is not only application where images are widely used for complete the application process, there are so many application available which have this kind of system. So, looking towards confidentiality of images it is very important to encrypt them in such a manner where no one can read the information inside it.So, in this era of hi-technology, looking towards the usage of images and threats, encryption of images is very important.

In the past decade, as the use of images was increased, threats increased and to overcome these threats few encryption methods were also introduced to keep the image safe. But, as the technology is changing every hour, so refinement of existing encryption methods is necessity of time. In the beginning, chaotic encryption technique [4] was introduced which was good on both type of images i.e. grey scale images and coloured images. But, due to its easy technology of just shifting pixel from its position in horizontal and vertical

direction to disorder the pixels from its original position in a predefined manner, this methodology was easier to crack and hence more confusing property need to be added in it. So, sticking on only one method is not safe in current scenario as hackers keep them updated with current technology and this reason motivates researchers to continuously improve the encryption methods time to time.

2. EXISTING APPROACHES

Chaotic Method [5]: This method is based on moving the complete pixel in horizontal and vertical direction based on some predefined key which is known to sender and receiver in advance. Pixels shifts first in horizontal direction followed by vertical direction and jump factor between pixels is again depending on the key. To increase the confusing in encrypted image, horizontal and vertical shifting performed more than once and number of time shifting is performed is kept confidential. But in this method one thing was movement of complete pixel from its position, so original colour and value of pixel remain same and decryption of same was not more than a tiny puzzle for hacker. So, this method could not successful in image encryption.

Bit Shifting: This is another method for image encryption which does not deal with shifting of pixel from its position as like in chaotic method. This method more focus on shifting of bits [6] either left shift or right shift within pixel based on some key and this is known as Secure Image Encryption. Shifting bits of pixel leads to change in colour of pixel which creates confusion for hacker to decrypt the image but pixel movement is also necessary to increase the difficulty for decryption. Manipulation of bits value is not enough because either left shift or right shift will give the result after few tries if pixel did not shifts from its position. So, more difficulty features need to be added in this feature.

Inter-Pixel Displacement:In this method focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method. In the similar manner, G and B values of pixel also shift from its position in both direction and jumping factor depends on confidential key. Number of horizontal and vertical manipulation of values depend on key and gap between pixel is also defines from key. So, key value increases in this case because it contains dual value, one for gap between pixel and second for number of horizontal and vertical movement order.Hence, in this method the RGB value of pixel goes to different positions which is most difficult for anyone to retrieve original image.

Considering the inter pixel displacement method which talks about the inter pixel displacement of RGB values in circular manner in both horizontal and vertical direction. Circular shift is performed in such a way that loss of RGB values is 0. For example is image is of dimension 1600*1200 or of any dimension and key value is 50 for R then first R value will be in 51 column and 2nd R value will be in 52 column and so on so forth. Similarly, for 1551 column the R value will jump into first column of image. Same circular fashion repeats with G and B but with different key value and same pattern repeats in vertical shift. But drawback of this method is continuous working of algorithm on whole image in one go. Hence, in improvement of this method, slicing scheme was introduced where one image is divided into few slices and then algorithm was applied which lead to more confusing property in encryption method.

3. PROPOSED METHOD

The proposed method is derived from the slicing [8] scheme of inter pixel displacement of RGB value because that has drawback of making slices from centre of image. So, if hacker knows that image is sliced from centre then decryption will be bit easy even though it still has other confidential properties. So, to improve this strategy further we can add more parameters to it. In the proposed method, centre point is not taken to slice the image. Any random point is taken using the rand() function in Matlab and this rand value is added to key. Now on the basis of this random value, image is sliced into 4 segments and base algorithm is applied on each quadrant of image.

Base algorithm [7] states that, each quadrant of image is first shuffled with the neighbouring quadrant then inter pixel displacement algorithm is applied on each quadrant independently. But, in our this new proposed algorithm, all these methods will be perform as it is and addition to that once each quadrant is finish with horizontal and vertical shifting of RGB inter pixel value then again the random point will be calculated and same process is applied again recursively. Architecture of same has been shown in figure 3.1.

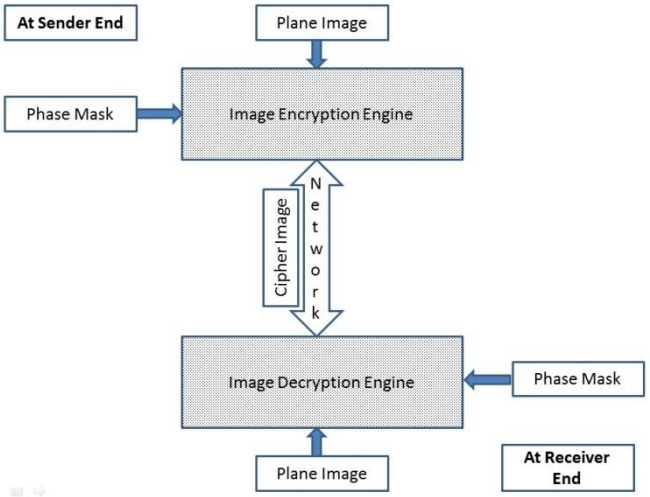

Figure 3.1 Architecture for Image Encryption.

So, the key value will consist of ordering of horizontal and vertical shifting which is also called mask for shifting, RGB key value which is different for all three, and the random value which is again different for each time and number of random points taken. Hence, in this way we are moving towards the big key size and key size directly proportional to difficulty in decryption of image. Small key size means less number of attempts to get the result and large key size means more number of attempts to get the result. For example, a key size of 3 bits can be cracked by maximum in 8 attempts and 5 bit key can be cracked in 32 attempts.

4. ALGORITHM

Image_Encryption()

1 : Img = any image of pixel x,y

2 : key=RMask

3 : loop while key >=1

Img=Slicing(Img,x,y)

End Loop

4 : End

This function will take any image which has to be encrypt as Img and RMask is a value which states that how many times this algorithm will run. For each value of key, slicing function will be called with the result received from last iteration.

Slicing (e, xmax, ymax)

1: e is An Input Image img with x coordinates 1 to xmax

2:xy[] = rand(); cx= xy[1]; cy[2].

3: Y coordinates 1 to ymax

3: Initialize quad=1, e=img

4: Loop while quad<=4

4.1 if quad=1

4.2 x1=1, x2=cx, y1=1, y2=cy

4.3 else if quad=2

4.4 x1=1, x2=cx, y1=cy+1, y2=ymax

4.5 else if quad=3

4.6 x1=cx+1, x2=xmax, y1=1, y2=cy

4.7 else

4.8 x1=cx+1, x2=xmax, y1=cy+1, y2=ymax

4.9 Invoke PerformEncryption(e,x1,x2,y1,y2,quad)

4.10 Increment quad by 1

4.11 EndLoop

5: Terminate

Slicing function will first find the random point to slice the image into four parts then on basis of that point; image will be divided into four quadrants. Earlier approach had fix point slicing of image from centre. This function will divide the image every time when this will call recursively. This function will call to PerformEncryption() function for each quadrant.

The PerformEncryption() method takes each of the quadrants with their coordinate limits and started performing the encryption process by deploying the shifting of R G B components among the pixels. The PM[] array called as Shift pattern mask array consists of binary digits 1's and 0's. The length of this array is the total number of vertical and horizontal shifts done in the encryption process. Each 1 triggers a circular vertical shift and a 0 triggers the invocation of circular horizontal shift. The PM[ ] can be made a part of the key or else supplied separately. With the increase in the length of the mask, the security as well as running time for encryption process increases linearly.

PerformEncryption (e,x1,x2,y1,y2,quad)

1: Supply PM[ ] array

1.1: Initialize Counter=1, initJump= Any Arbitrary Integer

1.2: Loop while PM[counter] is not NULL

1.2.1: if PM[counter]=0

InvokeHORIZONTAL_Shift(e,x1,x2,y1,y2,αr[counter],αg[counter], αb[counter],quad)

Increment counter by 1.

Endif

1.2.2: if PM[counter] = 1

Invoke VERTICAL_Shift(e,x1,x2,y1,y2, αr[counter], αg[counter], αb[counter],quad)

Increment counter by 1.

Endif

Endloop

2: Terminate

The PerformEncryption() method uses another set of arrays namely αr[counter], αg[counter], αb[counter] which holds in it the different integers for R, G and B component shifts. 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 colour component and hence it becomes a favourable condition for the cryptanalyst since guessing the shift of a single row is enough to know by how much are the other rows also shifted. The same entity is also used in the HORIZONTAL_Shift function also to provide a wider scattering of the R G B components from its native pixel position.

VERTICAL_Shift(e,x1,x2,y1,y2, α_r[counter], α_g[counter], α_b[counter],quad)

1: Input image with its coordinate limits x1 to x2,y1 to y2.

2: αr[counter], αg[counter], αb[counter]

3: ΔR= initJump + αr[counter]

4: ΔG= initJump + αg[counter]

5: ΔB= initJump + αb[counter]

6: Loop and Repeat steps for ColC = x1 to ColC= x2

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

ΔR = ΔR + αr[counter]

ΔG = ΔG + αg[counter]

ΔB = ΔB + αb[counter]

Endloop

7: Return

HORIZONTAL_Shift(e,x1,x2,y1,y2, α_r[counter], α_g[counter], α_b[counter],quad)

1: Input image with its coordinate limits x0 to xmaxy0 to ymax.

2: αr[counter], αg[counter], αb[counter]

3: ΔR= initJump + αr[counter]

4: ΔG= initJump+ αg[counter]

5: ΔB= initJump + αb[counter]

6: Loop and Repeat steps for RowC = y1 to RowC= y2

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 at RowCth row by ΔB pixels

ΔR = ΔR + αr[counter]

ΔG = ΔG + αg[counter]

ΔB = ΔB + αb[counter]

Endloop

5. CONCLUSION

We saw the different image encryption methods in this paper which focused on the image encryption using different manner, and proposed concept was based on inter-pixel displacement and random point slicing recursively. This method resulted in more confusing feature into the encryption but still there is a room for further improvement. In the further extension of this work, one might think upon the partition of image on other parameters which will secure the encryption process and, so no one can judge what encryption technique was used.

6. REFERENCES

[1] Information available on internet via www at http://uidai.gov.in/index.php?option=com_content&view=article&id=153&Itemid=13.

[2] Information available on internet via www at http://www.expresscomputeronline.com/20070312/technology01.shtml.

[3] Information available on internet via www at http://ewh.ieee.org/r10/bombay/news5/Biometrics.htm.

[4] RashidahKadir, Rosdiana Shahril2 and MohdAizainiMaarof, "A modified image encryption scheme based on 2D chaotic map" 978-1-4244-6235-3/10/$26.00 ©2010 IEEE.

[5] MazleenaSalleh, Subariah Ibrahim & Ismail FauziIsnin, "Image Encryption Algorithm Based On Chaotic Mapping".

[6] Jinping Fan, Yonglin Zhang, "Color image encryption and decryption based on double random phase encoding technique", 978-1-4244-4412-0/09/$25.00 ©2009 IEEE.

[7] Reji Mathews, AmneshGoel, Prachur Saxena & 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.

[8] Amnesh Goel, Reji Mathews &Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.