Image Encryption Based on Inter-Pixel Displacement

Ritu Siwatch¹, Veepin Kumar²

¹M. Tech Scholar, CSE Deptt.
²H.O.D. CSE Deptt.

¹Om Institute of Technology &Management, Guru Jambheshwar University, Hisar (Haryana), India
²Om Institute of Technology &Management, Guru Jambheshwar University, Hisar (Haryana), India

Abstract - In this era of technological advancements, to avoid the misuse of confidential information and misuse by the unauthorized access we need an encryption approach for security of image data. Here we proposed an algorithm which breaks the pixel into constituents i.e. red, green and blue are scattered to spatial space of image so that, basic property of pixel lost and difficult to reform the original image unless each of RGB component are located and identified. This paper discusses different methods of pixel displacement like chaotic method, bit shifting and inter-pixel displacement but focuses mainly on algorithms based on inter-pixel displacement. In these methods we used pixel shuffling, shifting and slicing.

Keywords- Cryptography, inter-pixel displacement, slicing, shuffling, shifting.

I. INTRODUCTION

As we all know that in this era of technology everyone has the access to the internet. So, we uses internet for the purpose of data transfer and this data may be in the form of textual or multimedia like audio, video and images etc. In these days we have many applications of internet in the field of military, government, private business, financial institution, multimedia system, telemedicine, financial status, e-commerce, online transaction processing, banking etc. Due to advancement of technologies mostly data transfer over the internet takes place in the form of sensitive images. And because the internet is vulnerable medium so we need to keep our information confidential, private and secure. We want that only the intended person will see the content. So certain precautions have to be adopted in handling the transfer of sensitive information over the internet.

Cryptography is the mechanism used for the security purpose of information. Cryptography is the art and science of safeguarding the documents or information so the only the intended people are able to visualize the contents. Cryptography provides us the main objectives like confidentiality, authentication, integrity and non-repudiation of information. Cryptography is beneficial but at the cost of some resources like CPU time, memory and encryption time. Cryptography comprises of two processes i.e. encryption and decryption. Encryption is the process of encoding a message i.e. converting plain text into cipher text and decryption is the reverse process of encryption i.e. converting cipher text to plain text.

In this paper we are applying encryption on image data. Here we are considering various methods of encryption based on different schemes because as attackers update their technique of decryption we have to come up with new techniques of encryption with high level of security.

As the images are made up of pixels and each pixel has three constituent part i.e. RGB. Pixel is the smallest element of image but still contain properties of image. So, here we are discussing encryption methods based on pixel. One of the methods was chaotic method in which the entire pixel shifted across rows and columns. But this method has limitation to colour images so another method developed in which pixel is further split up into its RGB component. These values denote the intensity level of RGB ranging from 0-255. All three components worked upon by algorithm with three different keys and scattered the native RGB component of one pixel into another. So, it was difficult to guess something about the pixel. Here we are reviewing some schemes based on this method.

Fig. 1 Encryption Decryption Process
A. Classification

Here we have classified various methods of encryption based on different algorithms. But as the technology is advancing and our need also. So, we need a strong method of encryption against all possible attacks.

1) Chaotic Method: 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 [5]. 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 [4]. So, this method could not successful in image encryption.

2) 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 either left shift or right shift within pixel based on some key and this is known as Secure Image Encryption [6]. 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 [7]. So, more difficulty features need to be added in this feature.

3) 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 [6]. 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 [7]. 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 [8]. 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 [6]. But drawback of this method is continuous working of algorithm on whole image in one go. Hence, there is need of some improvement.

II. PROPOSED ALGORITHMS

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

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 (Size = SumOfValuesRGB_cipher – SumOfValuesRGB_plaintext =0) [6]. Hence it is obvious that there 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 [3]. The pixel is the smallest element of an image which can be isolated and still contains the characteristic found in the image [3]. 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 [6]. 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.

Fig. 2. The proposed inter-pixel shift encryption scheme.

\[\alpha_r, \alpha_g, \alpha_b\] : 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 [8]. 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 favourable 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 [7]. Each 1 represents a circular vertical shift and a 0 initiates a circular horizontal shift. The PM[] can be derive 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.

B. A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement

Proposed image encryption method completes in two steps i.e. pixel rearrangement within image using sorting method and in second step image is encrypted using inter-pixel displacement algorithm. For the pixel rearrangement, all the pixels of image are first stored in an array where array sorting is performed. By the sorting method, all the pixels are get compound sort in ascending order of any value i.e. R, G, B and the top we gets 0, 0, 0 pixel if present and 255, 255, 255 in the last position if present [3]. Precedence of sorting is independent of value i.e. R, G, B because the motivation for sorting was reducing the correlation between pixel values [8]. This correlation method by arranging the pixel values in sorting order is better than block shifting.

This array which consists of sorted pixel on basis of RGB value is back transferred to form an image of original length and width size which will then have pixels in ascending order starting from 0, 0, 0 to 255, 255, 255 (both pixel are subject to present in plain image) [3]. Now, this image is used for the encryption purpose using the explosive inter-pixel displacement algorithm [8].

C. Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices

Considering the prime weakness in the above method, we propose a new technique to this problem in which instead of considering the whole image as one to work upon, we slice the images into n number of parts and the above method is applied to each of these slices separately [10]. Each size can be customized separately by choosing the number of rows and columns which in turn can be derived from the encryption keys. The secrecy factor introduced here provides a strong resistance against the multiple available alternatives for a single value of key [7]. To add to the security, the proposed method also induced the shuffling of the custom slices by inter changing the location of these slices from its actual image place location to different location repeating the shift algorithm with the new arrangement of the slices [10]. Changing the location of slices adds to the confusion for the cryptanalyst who is not provided with the knowledge of where and how the shuffling is performed and what is the updated location of each slice at that stage of the process.

Here we arbitrarily take the number of slices generated ‘n’ at each slicing process as 4 for the purpose of simulation and easier understand ability in the algorithm [7]. Once the slices are updated with new positions, a difference slice dimension can be applied to the current image making further split of the previous slices into further pieces. In this way, we
can achieve considerable amount of security in the ciphered image by dynamically deciding at each stage of how many more slicing and shuffling should be done. Hence we can custom the security levels and maintain a good trade off between the security and the running time complexity of the encryption and decryption process.

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

The proposed method is derived from the slicing scheme of inter pixel displacement of RGB value because that has drawback of making slices from centre of image [7]. 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 [10]. 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 states that, each quadrant of image is first shuffled with the neighbouring quadrant then inter pixel displacement algorithm is applied on each quadrant independently [9]. 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.

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 [10]. 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 4 bits can be cracked by maximum in 16 attempts and 6 bit key can be cracked in 64 attempts.

III. CONCLUSION

In this paper, image encryption using different manner reviewed but purposed concept based on inter-pixel displacement and random point slicing. Due to the extra slicing and shuffling this encryption scheme is more effective and provide large key space. Because of the strong key, it provides the great security to various applications which may include Bulk Encryption, Random Key Generation, Network Security and Internet based security.

REFERENCES