ISSN:0975-9646

New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique

Keerti Kushwah, Sini Shibu
Computer Science and Engineering
NIIST , Bhopal , India

Abstract: **The need of innovative encryption technique motivated us to develop this new image encryption algorithm named "New Image Encryption Technique based on Combination of Block Displacement and Block Cipher Technique" proposed by analyzing the principle of the image encryption algorithm. This will provide authorization of users, integrity and safety of images which is traveling over internet. Moreover, an image-based data requires more effort during encryption and decryption. This research introduces an image encryption algorithm which is the combination of "block displacement" and "Block Cipher. The original image was divided into blocks, which is then displaced horizontally and vertically and then resultant image will be divided into pixel blocks. This pixel block will be converted into binary value. Similarly key value will be selected. This key value will be converted in binary form. Finally key value will be XORed with Image value through proposed block based algorithm. Now finally encrypted image will be obtained. The Proposed Algorithm for encryption and decryption of an image using suitable user-defined key is developed. The cipher image generated by this method can vary in size with the original image due to image scaling to make 128 bits block at a time and is suitable for practical use in the secure transmission of confidential information over the Internet.**

Keywords : Security, Image, Network, Algorithm, Key

I. INTRODUCTION

The concept of image security and the word cryptography [12, 13] might be intimidating and complicated. The objective of the research is to develop a technique with tool that mediates the user and their operations to achieve image security goals. A platform independent tool with user-friendly graphical user interface, using already existing techniques and algorithms for cryptographic operations will be resulting product. People need to use the cryptographic operations in order to keep the personal image to avert from attackers in consideration of the security goals. These operations include algorithms consisting of various steps to protect the attacks of an attackers to reach and read personal images that is located in personal computer [24, 25]. Cryptographic operations consist of encryption and decryption techniques in computer and computer networking. The features which are in the scope of the proposed research to be developed are

- Encryption / Decryption Operations
- Authorization
- Key management

Rest of the Paper is organized as follow: Section II is the existing work. In this section the related work is studied Section III is problem identification and problem definition. In this the problem with existing image encryption is evaluated and these problems would be tried to overcome in proposed algorithm. Section IV is proposed work. In this section proposed concept about image encryption is presented. Section V is of results analysis. Finally Section VI is of conclusion. In this section overall conclusion of the paper are presented.

II. EXISTING STUDY

Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel,2012 by Amnesh Goel and Nidhi Chandra have investigated that if the image which is to be encrypted is firstly passed through a displacement process, which involves horizontal and vertical displacement, before applying encryption process, result in good encrypted image as compared to encrypting images directly. In this paper, in the First step original image is divided into blocks of n*n sizes which were rearranged using a transform algorithm presented in this paper. This transform image is now used for encryption rather than applying encryption procedure on plain image. This transformation of blocks reduces the correlation between the adjacent pixels and increases the entropy. This algorithm is being tested by making blocks of different sizes and then their result is being analysed [1].

Image Encryption Using Affine Transform and XOR Operation,2011 by Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar have investigated that image and text data are different from each other due to their unique features. In this article, we propose a new location transformation based encryption technique. Initailly pixel values are redistributed to different location using affine transform technique by using four 8-bit keys. This transformed image is then divided into 2 pixels x 2 pixels blocks and then each block is encrypted using XOR operation by using four 8-bit keys. The total key size used in this algorithm is 64 bit which proves to be strong enough. The experimental results showed and proved that after the affine transform the correlation between pixel values was decreased [2]

.

III. PROBLEM IDENTIFICATION AND PROBLEM DEFINITION

From the study of research paper I have conclude that in there are no clarifications of what format of RGB images they are using to perform image encryption and decryption procedure. I have also analyzed that there is no clarification about the configuration of machine. From further study I analyzed that Images are different from text. Although user may use the traditional cryptosystems to encrypt images directly, it is not a right idea for two reasons. One is that the size of image is almost always much higher than that of text. Therefore, the traditional cryptosystems need too much time to directly encrypt the image data. Another problem is that the decrypted text must be equal to the original or plain text. However, this requirement is not necessary for image data.

IV. PROPOSED WORK

In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). In order to dissipate the high correlation among pixels and increase the entropy value a newly designed image encryption algorithm titled "New Image Encryption Technique based on Combination of Block Displacement and Block Cipher Technique". This can be used in authorization of users and to verify integrity, accuracy and safety of images which is traveling over internet. Moreover, an image-based data requires more effort during encryption and decryption. This research introduces a block-based algorithm which is a combination of "Block Displacement" and "Block Cipher" based image encryption algorithms. The original image was divided into blocks, which is then displaced horizontally and vertically and then resultant image will be divided into pixel blocks. This pixel block will be converted into binary value. Similarly key value will be selected. This key value will be converted in binary form. Finally key value will be XORed with Image value through proposed block based algorithm. Now finally encrypted image will be obtained.The architecture for encryption and decryption of an image using suitable user-defined key is proposed and developed in this work. The cipher image generated by this method can vary in size with the original image due to image scaling to make 128 bits block at a time and is suitable for practical use in the secure transmission of confidential information over the Internet. By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to existing algorithm and thus improving the security level of the encrypted images.

A. *Block Diagram of Proposed Concept:*

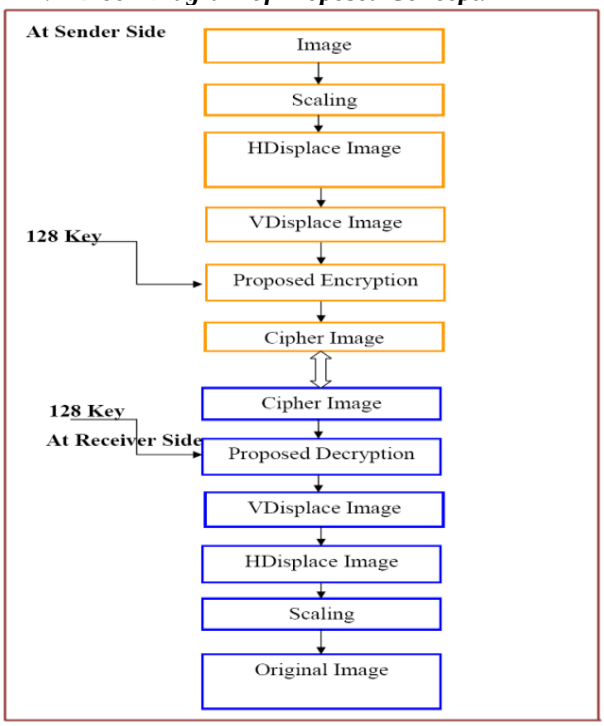


Figure 2.1: Block Diagram of Proposed System

Unlike in the previous research where the encryption algorithm is applied directly on the plain image, in this proposed scheme of image encryption there is some modification; In the First step original image is scaled and divided into blocks of n*n . This scaled image is now used for encryption. The scaling is performed in order to make the block size of n*n of an image. The displacement of blocks reduces the correlation between the adjacent pixels and increases the entropy. This algorithm is being tested by making blocks of different sizes and then their result is being analyzed [1].

```
DisplaceAlgoHorizontal(image)
1:img=image //input plain image
2:bSize=enter block size
3:rows=image(1); cols=image(2)
4:hBlock=rows/bSize; vBlock=cols/bSize
5:for i=1 to vBlock
for j=1 to hBlock
Move Blocks in reference of 1
End For
EndFor
Invoke DisplaceAlgoVertical(image)
End
```

DisplaceAlgoHorizontal(image) will identify the number of horizontal and vertical blocks in an image and accordingly it will explosively displace the blocks in horizontal direction in the 1:1 manner; according to this method, block at location 1st will to 2nd block position, 2nd block will move to 3th block position and 3rd block will move to 4th block position. Similarly block at location 4^{th} will to 3^{rd} block position, 3^{rd} block will move to 2^{nd} block position and 2^{nd} block will move to 1^{st} block position. This displacement of blocks is exchange which further means that there will be no loss of data in displacement. Number of pixels in a block will be determining by bSize, rows and cols are the number of rows and number of cols in the image. After performing the horizontal block displacement, this will invoke the another method DisplaceAlgoVertical(image) [1].

```
DisplaceAlgoVertical(image)
1:img=image
2:bSize=enter block size
3:rows=image(1); cols=image(2)
4:hBlock=rows/bSize; vBlock=cols/bSize
5:for i=1 to hBlock
for j=1 to vBlock
Move Blocks in reference of 1, 2, 3
End For
EndFor
Invoke PerformEncryption(image,rows,cols)
End
```

DisplaceAlgoVertical(image) will work in the same manner as of DisplacAlgoHorizontal(image) method, but this will displace the blocks in the vertical direction instead of horizontal direction. Rest of functionality is same as per previous method. After performing vertical displacement of blocks, this will invoke the PerformEncryption() method [1].

B. Proposed Encryption/Decryption:

Proposed Encryption :

1. Input Key (K) 128 bits.
2. Divide K into four sub part of equal size
   K_1, K_2, K_3, K_4 {32 bits each}
3. Input an Image (I)
4. Read total number of pixel value of I.
   P_i (I) {i = 1, 2, 3,… …n
5. Convert P_i (I) into binary value.
   Binary (P_i (I))
6. Repeat following steps till Binary (P_i (I)) ! = NULL
7. Read first 128 bits binary value of (P_i (I))
8. Divide (P_i (I)) into four sub part of equal size
   P_1, P_2, P_3, P_4 {32 bits each}
9. Select P_1 and apply reverse operation to produce (P_5).
   P_1 —Reverse→ P_5
10. Perform XOR between P_5 & P_2 to produced (P_6).
    P_5 XOR P_2 ⟶ P_6
11. Select P_5 and apply 2 bits right circular shift to produce P_{11}.
    P_5 —(>>)→ P_{11}
12. Select P_3 and apply 2 bits left circular shift to produce (P_7).
    P_3 —(<<)→ P_7
13. Perform XOR between P_7 & P_6 to produced (P_8).
    P_7 XOR P_6 ⟶ P_8
14. Select P_4 and apply reverse operation to produce (P_9).
    P_4 —Reverse→ P_9
15. Perform XOR between P_9 & P_8 to produced (P_{10}).
    P_9 XOR P_8 ⟶ P_{10}
16. Perform XOR between P_{10} & P_{11} to produced (P_{12}).
    P_{10} XOR P_{11} ⟶ P_{12}
17. Select K_1 and perform XOR with P_{12} to produce (C_1).
    K_1 XOR P_{12} ⟶ C_1
18. Perform XOR between C_1 & P_6 to produce (P_{13}).
    C_1 XOR P_6 ⟶ P_{13}
19. Select K_2 and perform XOR with P_{13} to produce (C_2).
    K_1 XOR P_{13} ⟶ C_2
20. Perform XOR between C_2 & P_8 to produce (P_{14}).
    C_2 XOR P_8 ⟶ P_{14}
21. Select K_3 and perform XOR with P_{14} to produce (C_3).
    K_1 XOR P_{14} ⟶ C_3
22. Perform XOR between C_3 & P_{10} to produce (P_{15}).
    C_2 XOR P_{10} ⟶ P_{15}
23. Select K_4 and perform XOR with P_{15} to produce (C_4).
    K_4 XOR P_{15} ⟶ C_4
24. Now finally concatenate to (C_1, C_2, C_3 and C_4) to produce final cipher value (CP_i)
25. Exit.

Proposed Decryption:

1. Input Key (K) 128 bits.
2. Divide K into four sub part of equal size
   K_1, K2, K_3, K_4 {32 bits each}
3. Input an Cipher Image (CI)
4. Read total number of pixel value of CI.
   P_i (CI) {i = 1, 2, 3,… …n
5. Convert P_i (CI) into binary value.
   Binary (P_i (CI))
6. Repeat following steps till Binary (P_i (CI)) ! = NULL
7. Read first 128 bits binary value of (P_i (CI))
8. Divide (P_i (CI)) into four sub part of equal size
   C_1, C_2, C_3, C_4 {32 bits each}
9. Select K_4 and perform XOR with C_4 to produced (P_{15}).
   K_4 XOR C_4 ⟶ P_{15}
10. Perform XOR between P_{15} and C_3 to produce (P_{10}).
    P_{15} XOR C_3 ⟶ P_{10}
11. Select K_3 and perform XOR with C_3 to produced (P_{14}).
    K_3 XOR C_3 ⟶ P_{14}
12. Perform XOR between P_{14} and C_2 to produce (P_8).
    P_{14} XOR C_2 ⟶ P_8
13. Select K_2 and perform XOR with C_2 to produced (P_{13}).
    K_2 XOR C_2 ⟶ P_{13}

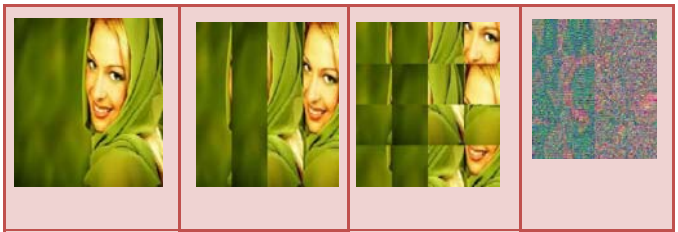
14. Perform XOR between P_{13} and C_1 to produce (P_6).
    P_{13} XOR C_1 ⟶ P_6
1. Select K_1 and perform XOR with C_1 to produced (P_{12}).
    K_1 XOR C_1 ⟶ P_{12}
2. Perform XOR between P_{12} & P_{10} to produced (P_{11}).
    P_{12} XOR P_{10} ⟶ P_{11}
3. Perform XOR between P_6 & P_8 to produced (P_7).
    P_6 XOR P_8 ⟶ P_7
4. Perform XOR between P_{10} & P_7 to produced (P_9).
    P_{10} XOR P_7 ⟶ P_9
5. Select P_7 and apply reverse left circular shift to produce (P_3).
    P_7 —Rev (<<)→ P_3
6. Select P_9 and apply reveres operation to produce (P_4).
    P_9 —Reverse (P_9)→ P_4
7. Select P_{11} and apply reverse right circular shift to produce (P_5).
    P_{11} —Rev (>>)→ P_5
8. Perform XOR between P_5 & P_6 to produced (P_2).
    P_5 XOR P_6 ⟶ P_2
9. Select P_5 and apply reverse operation to produce (P_1).
    P_5 —Reverse (P_5)→ P_1
10. Now finally concatenate (P_1, P_2, P_3, P_4) to produce original pixels value.
11. Exit

V. RESULTS

The figures and tables shown below shows the experimental results done on images of size 200x200, 240x240 and 240x240 by taking block size of 100,60 and 40 respectively.

Scaled Image	Horizontal Displaced Image	Vertical Displaced Image	Encrypted Image

Figure 5.1:Case-I: Image 1.jpg 200 X 200 Block Size 100



Scaled Image	Horizontal Displaced Image	Vertical Displaced Image	Encrypted Image

Figure 5.2: Case-II: Image 2.jpg 240 X 240 Block Size 60

Scaled Image	Horizontal Displace Image	Vertical Displace Image	Encrypted Image

Figure 5.3: Case-III: Image 3.jpg 240 X 240 Block Size 40

Images	ENTROPY
Image1.jpg(200x200)	508.255
Image2.jpg(240x240)	493.7579
Image3.jpg(240x240)	507.439

Table 5.1 Encrypted Images Entropy on Block Size 100,60 and 40 respectively

Images	CORRELATION
Image1.jpg(200x200)	0.0541
Image2.jpg(240x240)	0.1710
Image3.jpg(240x240)	0.0192

Table 5.2 Encrypted Images correlation on Block Size 100,60 and 40 respectively

VI. CONCLUSION

In this paper, a new image encryption algorithm is proposed. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed algorithm used 128 bits key length which is provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2^{128} time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formula have applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm was calculated.

REFRENCES

[1] Amnesh Goel and Nidhi Chandra, *A Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel*, 2012 IEEE International Conference on Communication Systems and Network Technologies, pp 884 – 888, 11-13 May 2012

[2] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar ,*Image Encryption Using Affine Transform and XOR Operation* "Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011),pp 309 – 312, 21-22 July 2011

[3] D. Chattopadhyay, M. K. Mandal and D. Nandi ,*Robust Chaotic Image Encryption based on Perturbation Technique,* published in ICGST-GVIP Journal, Volume 11, Issue 2,pp.41-50 April 2011

[4] Manjunath Prasad1 and K.L.Sudha2a,"*Chaos Image Encryption using Pixel shuffling* published in D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011.

[5] Jolly Shah and Dr. Vikas Saxena,*Performance Study on Image Encryption Schemes* published in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1,pp 349-355, July 2011 ISSN (Online): 1694-0814.

[6] Reji Mathews, Amnesh Goel and 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, pp. 8-11,December 2011

[7] William stallings, "Cryptography and Network Security:Principles & Practices", second edition

[8] Introduction of cryptography by H. Delfs and H. Knebl springer verlag berlin Heidelberg 2007

[9] William Stallings "Cryptography and Network Security",3rd Edition, Prentice-Hall Inc., 2005

[10] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C", John Wiley and Sons, Inc., 1996.

[11] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994

[12] B. Schneier, "Data Guardians," MacWorld, Feb 1993, 145-151