ISSN: 2278-5213

RESEARCH ARTICLE

# Advance Cryptography Algorithm for Symmetric Image Encryption and Decryption Scheme for Improving Data Security

**K. Ganeshkumar*, D. Arivazhagan and S. Sundaram**
Dept. of Information Technology, AMET University, Chennai, India
arivazhagand@hotmail.com, ganesheclipse@gmail.com*; +91 9790525505

## Abstract

Nowadays all activities are performed through online only. We cannot give substantiation of security to the data, so we are using one major method to defend our data while sending it through internet called cryptography. After analyzing several digital encryption and decryption algorithms this study designs a symmetric image encryption and decryption scheme based on the RGB colors and blowfish encryption algorithms. Through number of experimental tests conducted with this detailed encryption algorithm, we demonstrate a high security algorithm of the new scheme. In this study, we propose a new algorithm to encrypt an image for secure transfer. At the start, we break up the colors of the original image using coloring algorithm, the colors are red, blue and green so we get three images having three kinds of colors. Each color image is divided in to vertical and horizontal blocks, the number of blocks based on the size of the image. Each block is numbered and they are rearranged using blowfish algorithm. After rearrangement, the 128 bit public key is added to the colored image. Finally the three colored images are combined together and it forms a chipper image. This encryption algorithm gives more correlation effect compared to previous encryption algorithms.

**Keywords:** Encryption, decryption algorithms, data security, cryptography, RGB colors, blowfish algorithm.

## Introduction

Encryption is the process of transforming the original data in to a chipper data (the original data can be transferred to unreadable format) and converting the chipper data to original data in other side (Kiran Kumar *et al.*, 2010). With the enormous growth of computer networks and digital technologies, a huge amount of digital images are transferred through networks. Mostly the images from bank transaction and any money related digital images will be confidential or private, distinct security algorithm has been used to provide the required protection methods (Abusukhon and Talib, 2012). The security of bank or money oriented images become more and more emphasis due to the high evolution of e-banking in the network world today (Guo *et al*., 2010). The security of these kinds of images has attracted more and many different image encryption algorithms have been proposed to enhance the security of checks and demand draft images (Liu *et al.,* 1993). This image encryption algorithm try to convert to another one, that can be hard to understand and hard to rearrange (Tao *et al.,* 1998). On the other hand, the encrypted image gets decrypted and bring original image. In recent years, we have various encryption and decryption algorithms and there is no single algorithm that satisfies different image types but can encrypt all type of images (Zhang and Liu, 2011). Most of algorithms are designed to encryption and decryption of original images which are proposed in the middle of 1990s.

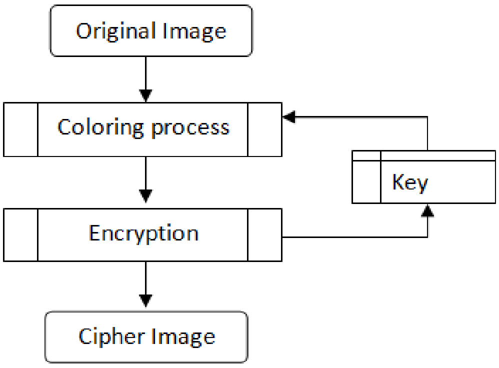
The encryption algorithm is classified in two ways one is non-chaos selective method and another is chaos based selective method (Zhao and Chen, 2002). Lakhtaria (2011) studied about protecting computer network with encryption technique with bit pixel and block permutations. Chan (2011) in his study on security framework for privacy preserving data aggregation in wireless sensor networks showed shuffling image pixels which changed the value of gray color of image and confused the hacker to find out the chipper text. Padma *et al.* (2010) in their study on encoding and decoding of a message in the implementation of elliptic curve cryptography provided secret combinations combined with other encryption techniques to make highly encrypted chipper images. Kiran Kumar *et al.* (2010) studied efficient digital encryption algorithm based on matrix scrambling technique, this image encryption based on the permutation of pixels combined with a new algorithm. Abusukhon and Talib (2010) in their study used digital signature algorithm to create a complex digital algorithm for making encryption. Cryptography is referred as encipher or encoding used to convert the image or text to incomprehensible format. When the data are to be transmitting, it will be decrypted depending on what kind of data to be sent. More and more important images like checks and tenders transmit over the internet due to the enormous growth of internet and multimedia technology (Lakhtaria, 2011).

A new approach is recommended in this study for fast and secure image encryption. In this study, we propose a new encryption algorithm based on the image encryption using color scheme encryption. The image values of blocks are strongly connected and the blocks are predicted by the values (Zaidan *et al*., 2010). We propose a coloring algorithm that divides the images by their colors, subdivide into blocks and shuffle their blocks position before it is transmitted by blowfish encryption algorithm. Before the encryption, we added the 128 bit public key for more encryption (Padma *et al.,* 2010). The secret key of algorithm is used to encrypt the shuffled image and check the correlation value, the value is very high compared with other encryption algorithms (Ganeshkumar *et al.,* 2013).

## Materials and methods

*Description of coloring algorithm:* The original image is divided in to three number of images based on RGB. After separating the color images, each and every image is subdivided in to horizontal and vertical blocks like Table. The blocks are having sequence number collapsed by blowfish algorithm and 128 bit public key was added to each color images to get the final chipper image. At the receiver side, the original image can be obtained by reverse transformation of the blocks. Here, we present the general block diagram of coloring method (Fig. 1).

Fig. 1. General block diagram of the coloring algorithm.



*Coloring algorithm:* The coloring algorithm is presented below. It generates a new chipper image based on the colors and their blocks.

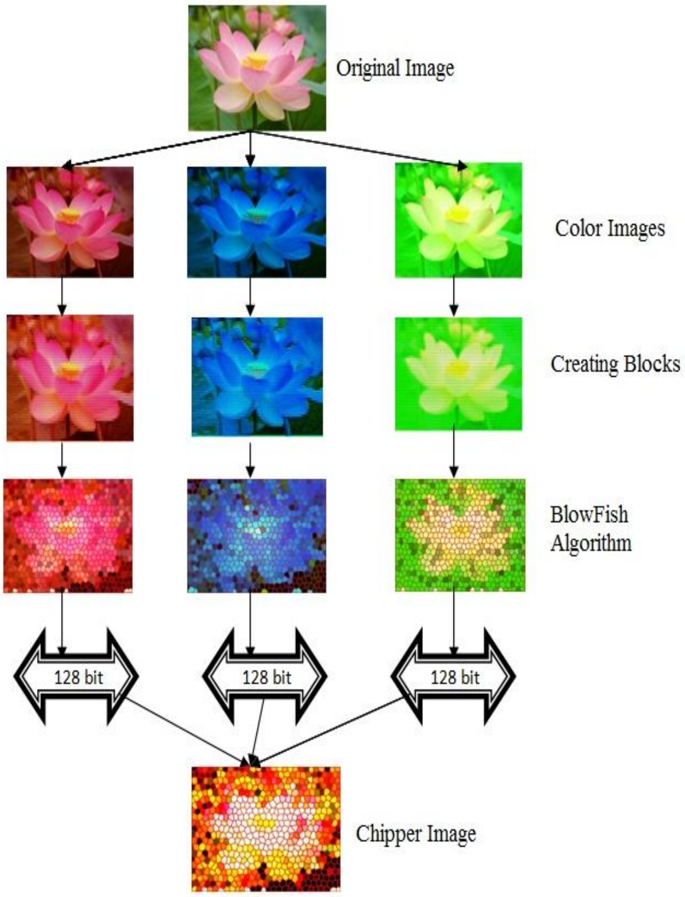
```
ALGORITHM CREATE_COLOR_ENCRYPTION_IMAGE
1: Load Image
2: Separation
        2.1: if(Pixel==red)
                        Separate red color
        2.2: if(Pixel==Blue)
Separate Blue Color
2.3: if(Pixel==Green)
Separate Green Color
2.4: HorizantalNoBlocks=Int(imagewidth/20)
2.5: VerticalNoBlocks=Int(imageheight/20)
2.6: Randamizattion()
2.7: RedColorImage=BlowFish(HorisantalNoBlocks,
VerticalNoBlocks)
2.8: greenColorImage=BlowFish(HorisantalNoBlocks,
VerticalNoBlocks)
2.9: BlueColorImage=BlowFish(HorisantalNoBlocks,
VerticalNoBlocks)
2.9.1: Add 128 public key to RGB image
2.10: Combine(Redcolorimage,GreencolorImage,
BlueColorImage)
2.11: End if
2.12: End if
2.13: End if
2.14: End CREATE_COLOR_ENCRYPT_IMAGE
```

*Description of combination technique:* The proposed color based encryption algorithm is based on the combination of colored encryption followed by the blowfish encryption techniques. The new proposed algorithm is used to produce three kinds of new colored chipper images from the original images.

a) Red color chipper image
b) Blue chipper image
c) Green color chipper image

These three images are encrypted using blowfish algorithm and after that we added a 128 bit key to the three colored images and merged the three images. The overview model of the proposed technique is shown in Fig. 2.

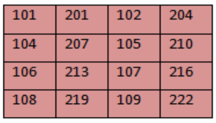
Fig. 2. Description of combination technique.



*Permutation process:* In this process, the position of the horizontal blocks and vertical blocks are changed by applying the following coloring algorithm (Chan, 2011).

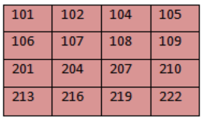
```
Function Ascending(Redcolor[row][col])
Begin
Set nsqur=no*no ,R=10,P=101,B=201
For(row=0;row<=nsqur;row=row+1)
{
    For(col=0;col<=nsqur;col=col+1)
    {
    Redcolor[row][col]=R
    R=R+1
    }
}
For(row=0;row<=nsqur;row=row+1)
{
For(col=0;col<=nsqur;col=col+1)
{
    If(Redcolor[row][col]%2==0)
    {
    Redcolor[row][col]=p
    P=p+1
}
End If
Ascending(value(REDCOLOR[row][col])
}
End
```

In the following example, how blocks are numbered and reshuffled with in colored images is shown. Blocks of sub-image of dimension 5x5 are shown below.



| | | | |
|---|---|---|---|
| 101 | 201 | 102 | 204 |
| 104 | 207 | 105 | 210 |
| 106 | 213 | 107 | 216 |
| 108 | 219 | 109 | 222 |

Assigning number

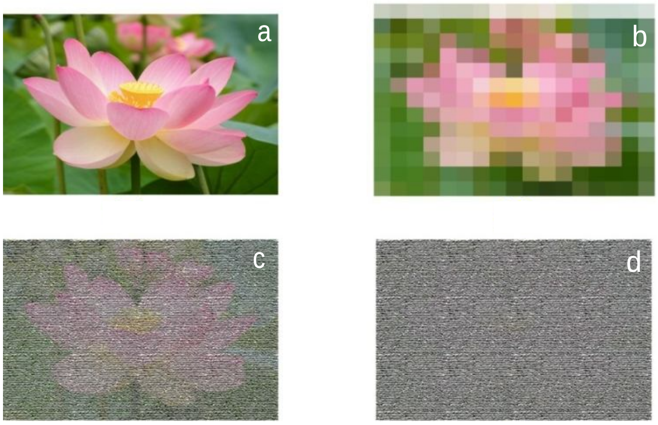


| | | | |
|---|---|---|---|
| 101 | 102 | 104 | 105 |
| 106 | 107 | 108 | 109 |
| 201 | 204 | 207 | 210 |
| 213 | 216 | 219 | 222 |

Reshuffling the blocks

*Experimental design:* The algorithm was applied in a MPEG image file that has a size of 20x20 block and three colors (Fig. 3a-d). The image is decoded in to 20x20 blocks. Here, we take an example of an image which is encrypted by our coloring algorithm (Wang *et al.,* 2011).

Fig. 3a. Original image, b. Red chipper image with blocks, c. After adding blowfish algorithm, d. Adding 128 bit public key.



We compared the colored algorithm with commonly used encryption algorithms namely blowfish, twofish and RC4 (Zhu *et al.,* 2011). These algorithms are commonly available, so we took that for comparison with our chipper text. In the next step, the correlation value of the chipper text was evaluated with the following formula:

$$r = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}}$$

r = Correlation value
n= Number of block of image
ΣXY = Sum of the product of first and Second blocks
ΣX = Sum of First blocks
ΣY = Sum of Second blocks
$\Sigma X^2$ = Sum of square First blocks
$\Sigma Y^2$ = Sum of square Second blocks

If the r value is very higher than other algorithms then we can consider our algorithm is better than other.

## Results and discussion

The result of our algorithm gave a very high complicated chipper image. This is made by the combination of two encryption algorithms namely coloring algorithm and blowfish algorithm. In this encryption method, we can encrypt any kind of images like JPEG, GIF and TIF etc. If we encrypt the image using other common encryption algorithms, the hacker may know the steps of the common algorithm and can easily identify the original image. When we use the new proposed coloring algorithm, the hacker may hack the chipper image but it is very tedious task to convert it into original image, because in our algorithm we separate the image in to vertical and horizontal blocks and the number of blocks depend upon the image size, so the hacker will not able to identify the number of blocks.

Table 1. Comparison of correlation value of proposed algorithm with common algorithms.

| Algorithm | Number of blocks | Correlation r value |
|---|---|---|
| blowfish | 30x30 | 0.0189 |
| | 60x60 | 0.0054 |
| | 100x100 | 0.0051 |
| | 300x300 | 0.0038 |
| Twofish | 30x30 | 0.0026 |
| | 60x60 | 0.0040 |
| | 100x100 | 0.0041 |
| | 300x300 | 0.0029 |
| Coloring | 30x30 | 0.0053 |
| | 60x60 | 0.0045 |
| | 100x100 | 0.0085 |
| | 300x300 | 0.0065 |
| RC4 | 30x30 | 0.0021 |
| | 60x60 | 0.0045 |
| | 100x100 | 0.0011 |
| | 300x300 | 0.0023 |

After getting the chipper image we calculated the correlation value of the chipper image. The correlation value of the coloring algorithm is very high compared to other common encryption algorithms, so the proposed algorithm is better than other encryption algorithms (Table 1). We can use our new proposed algorithm in any kind of banking applications and any government oriented websites for secured image transfer. New kind of encryption techniques may be added in this algorithm for further study.

## Conclusion

In this study, a clear and strong algorithm has been proposed for image encryption using a combination of color based encryption and blowfish algorithm. We investigated the efficiency of the proposed algorithm with other common available algorithms. It is good for image encryption in a network system and has a very good performance whenever the encrypted image is sent across the network. The correlation is increased in proposed algorithm when compared with other older algorithms and the proposed algorithm resulted in best performance because of the highest correlation.

## References

1. Abusukhon, A. and Talib, M. 2012. A novel network security algorithm based on private key encryption. In Proc. Int. Conf. on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec12), 2012. pp.1119-1224.
2. Chan, A. 2011. A security framework for privacy-preserving data aggregation in wireless sensor networks. *ACM Trans. Sensor Networks*. 7(5): 1-5.
3. Chen, G., Mao, Y. and Chui, C.K. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals.* 21(3): 749-761.
4. Ganeshkumar, K., Arivazhagan, D. and Sundaram, S. 2013. Strategies of cybercrime: Viruses and security sphere. *J. Acad. Indus. Res*. 2(7): 397-401.
5. Guo, Q., Liu, Z. and Liu, S. 2010. Color image encryption by using Arnold and discrete fractional random transforms in IHS space. *Optics Lasers Engg.* 48(12):1174-1181.
6. Huang, C.K. and Nien, H.H. 2009. Multi chaotic systems based pixel shuffle for image encryption. *Optics Commun.* 282(11): 2123-2127.
7. Kiran Kumar, M., Mukthyar Azam, S. and Rasool, S. 2010. Efficient digital encryption algorithm based on matrix scrambling technique. *Int. J. Network Security Appl*. 2(4): 30-36.
8. Lakhtaria, K. 2011. Protecting computer network with encryption technique: A Study. *Int. J. U-E-Serv. Sci. Technol.* 4(4): 44-51.
9. Liu, Z., Chen, H. and Liu, T. 1993. Image encryption by using gyrator transform and Arnold transform. *J. Elec. Imag.* 2(4): 345-351.
10. Padma, B.H., Chandravathi, D. and Roja, P.P. 2010. Encoding and decoding of a message in the implementation of elliptic curve cryptography using Koblitz's method. *Int. J. Computer Sci. Engg.* 2(5): 1904-1909.
11. Tao, R., Meng, X.Y. and Wang, Y. 2010. Image encryption with multiorders of fractional fourier transforms. *IEEE Trans. Information Forensics Security.* 5(4): 734-738.
12. Wang, X.Y., Yang, L., Liu, R. and Kadir, A. 2010. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynam.* 62(3): 615-621.
13. Wang, Y., Wong, K.W., Liao, X. and Chen, G. 2011. A new chaos-based fast image encryption algorithm. *Appl. Soft Computing J.* 11(1): 514-522.
14. Zaidan, B., Zaidan, A., Al-Frajat, A. and Jalab, H. 2010. On the differences between hiding information and cryptography techniques: An overview. *J. Appl. Sci*. 10: 1650-1655.
15. Zhang, G. and Liu, Q. 2011. A novel image encryption method based on total shuffling scheme. *Optics Commun*. 284(12): 2775-2780.
16. Zhao, X.Y. and Chen, G. 2002. Ergodic matrix in image encryption. *In Proc. of the 2nd Int. Conf. Image Graphics.* 4875: 394-401.
17. Zhu, Z.L., Zhang, W., Wong, K.W. and Yu, H. 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inform. Sci.* 181(6): 1171-1186.
18. Zunino, R. 1998. Fractal circuit layout for spatial decorrelation of images. *Elec. Lett*. 34(20): 1929-1930.