# RGB Color Image Encryption-Decryption Using Gray Image

**Ahmad A.M Sharadqah**[1]

[1] **Computer Engineering Department, Al-Balqa' Applied University, Amman**

**Abstract**

This paper presents a novel effective method for image encryption, which employs obtaining a gray image from the original image, then encrypting this image. The novelty of this method lies in deploying the concept of matrix multiplication for encryption-decryption purpose. The effectiveness of the proposed encryption method lies in minimizing encryption-decryption times and minimizing the mean square error between the original and the decrypted images. In recent years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access. The proposed method has high security features because the matrix key used for encryption-decryption is generated randomly and makes the process of hacking the matrix key very difficult.

***Keywords:*** *Direct conversion, Inverse conversion, HSI model, R'G'B' model, Encryption, Decryption, Matrix key, Encryption time, Decryption time, MSE***.**

## 1. Introduction

With the rapid growth of computer networks and advances in information technology, a huge amount of digital data is being exchanged over unsecured channels. Major part of transmitting information, either private or confidential, demands for security methods to provide required protection, therefore information security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of the network gradually leads us to acquire information directly and clearly through images [1]. Hence, image security has become a critical and imperative issue [2]. Image encryption methods try to convert an image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption [3] [4] [5]. Furthermore, special and reliable security in the storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications and confidential video conferences.etc. In order to fulfill such a task, many image encryption methods have been proposed, but some of them have been known to be insecure [5], so we always in need to develop more and more secure imagge encryption techniques. Traditional data encryption methods can be divided into two categories which are used individually or in combination in every cryptographic algorithm: substitution and transposition. In substitution technique, we symmetrically replace one symbol, in the data with another symbol according to some algorithm; in a transposition technique, we reorder the position of symbols in the data according to some rule [6].

This paper will focus in image encryption-decryption using matrix multiplication.

RGB color image can be encrypted-decrypted by converting color images to gray image using the HSI model as described in [7, 8, and 9], or using R'G'B' model proposed by the authors in [10,11, and 12].

## 2. Theoretical part

With the rapid growth of computer networks and advances in information technology, a huge amount of digital data is being exchanged over unsecured channels. Major part of transmitting information, either private or confidential, demands for security methods to provide required protection, therefore information security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of the network gradually leads us to acquire information directly and clearly through images [1]. Hence, image security has become a critical and imperative issue [2].

Color image can be encrypted-decrypted without any loss of information and with a high degree of security using matrix multiplication, here a huge matrix (or more) with a double type values can be generated to be used as an encryption key, this can be hardly hack able, and very difficult to guess. The key is a square matrix which must cover the image size.

In [10] [11] [12] an R'G'B' model was proposed to convert RGB color image to gray image. This model can be used also to encrypt-decrypt color image using the following steps:

1. Encryption phase:

   1.1 Get the original color image.

1.2 Use mathematical models to extract red, green, and gray images (apply direct conversion).

1.3 If the gray matrix is not square, resize the matrix.

1.4 Generate a matrix key with random numbers and size equal to the resized gray image matrix.

1.5 Apply matrix multiplication (gray matrix with the key) to get the encrypted gray image.

1.6 Resize the image using the original size.

1.7 Apply inverse conversion to reconstruct the encrypted color image.

2. Decryption phase:

2.1 Get the decrypted color image.

2.2 Use mathematical models to extract red, green, and gray images (apply direct conversion).

2.3 If the gray matrix is not square, resize the matrix.

2.4 Apply matrix multiplication (gray matrix with the inverse matrix key) to get the encrypted gray image.

2.5 Resize the image using the original size.

2.6 Apply inverse conversion to reconstruct the decrypted color image.

The same procedures are used to encrypt-decrypt color image using the HSI model, but direct and inverse conversions are implemented using the HSI mathematical model.

Also color image can be encrypted decrypted directly using the red, green, and blue components. Here the encryption-decryption process can be implemented according to the following steps

1. Encryption phase:

1.1 Get the original color image.

1.2 Extract red, green, and blue components of the color image.

1.3 If the component matrices are not square, resize them.

1.4 For each component generates a matrix key with random numbers and size equal to the resized component matrix.

1.5 Apply matrix multiplication (component matrix with the key) to get the encrypted red, green and blue images.

1.6 Apply matrices resizing if needed.

1.7 Reconstruct the color image to form, the encrypted image.

2. Decryption phase:

2.1 Get the decrypted color image.

2.2 Extract red, green, and blue components of the color image.

2.3 If the component matrices are not square, resize them.

2.4 Apply matrix multiplication (each component with its inverse matrix key) to get the encrypted image component.

2.5 Apply matrices resizing if needed.

2.6 Reconstruct the color image to form, the encrypted image.

## 3. Experimental part

A Matlab codes were written to implement the above three mentioned methodologies of color image encryption-decryption. The codes were tested using an IBM PC with i3 2,5 GHz processor and 4 Gbyte memory using different color images with different sizes. All the three methods give a mean square error (MSE) equal to zero and a 100% matching between the original image and the decrypted image. Figures (1) and (2) show a sample of using R'G'B' method of encryption.

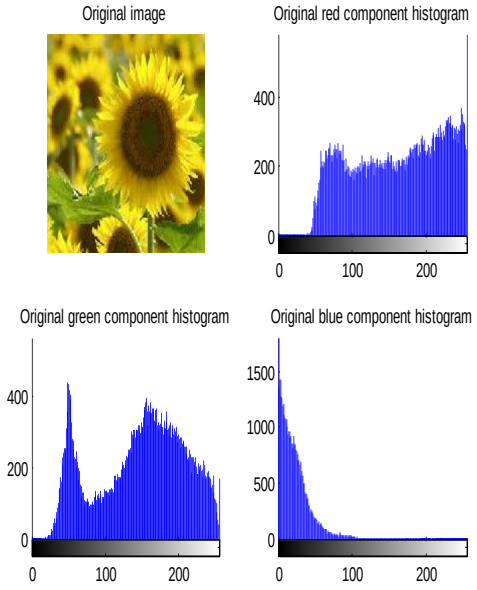


Fig 1. The original color image and histograms

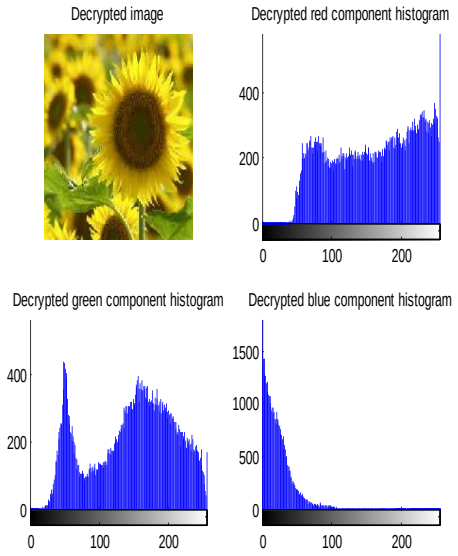


Fig 2. The decrypted color image and histograms

For performance analysis the required total time for encryption-decryption was measured for each color image and the results of measuring are listed in tables (1), (2), (3), (4) and (5).

Table (1): Measurement results using R'G'B' method for encryption time

| Encryption time | | | | |
|---|---|---|---|---|
| Image size | Direct conversion time(sec.) | Encryption time | Inverse conversion time | Total time |
| 256×320×3 | 0.015 | 0.0389 | 0.015 | 0.0689 |
| 384×512×3 | 0.016 | 0.0934 | 0.016 | 0.1254 |
| 227×303×3 | 0.015 | 0.0327 | 0.015 | 0.0627 |
| 300 ×500×3 | 0.015 | 0.0713 | 0.015 | 0.1013 |
| 480×640×3 | 0.031 | 0.1460 | 0.031 | 0.2080 |
| 1500×1200×3 | 0.313 | 0.8553 | 0.313 | 1.4813 |

Table (2): Measurement results using R'G'B' method for decryption time

| Decryption time | | | | |
|---|---|---|---|---|
| Image size | Direct conversion time(sec.) | Decryption time | Inverse conversion time | Total time |
| 256×320×3 | 0.015 | 0.0514 | 0.015 | 0.0814 |
| 384×512×3 | 0.016 | 0.1233 | 0.016 | 0.1553 |
| 227×303×3 | 0.015 | 0.0431 | 0.015 | 0.0731 |
| 300 ×500×3 | 0.015 | 0.0940 | 0.015 | 0.1240 |
| 480×640×3 | 0.031 | 0.1926 | 0.031 | 0.2546 |
| 1500×1200×3 | 0.313 | 1.1285 | 0.313 | 1.7545 |

Table (3): Measurement results using HSI method for encryption time

| Encryption time | | | | |
|---|---|---|---|---|
| Image size | Direct conversion time(sec.) | Encryption time | Inverse conversion time | Total time |
| 256×320×3 | 0.094 | 0.0389 | 0.031 | 0.1639 |
| 384×512×3 | 0.188 | 0.0934 | 0.094 | 0.3754 |
| 227×303×3 | 0.078 | 0.0327 | 0.032 | 0.1427 |
| 300 ×500×3 | 0.078 | 0.0713 | 0.079 | 0.2283 |
| 480×640×3 | 0.157 | 0.1460 | 0.125 | 0.4280 |

Table (4): Measurement results using HSI method for decryption time

| Decryption time | | | | |
|---|---|---|---|---|
| Image size | Direct conversion time(sec.) | Decryption time | Inverse conversion time | Total time |
| 256×320×3 | 0.094 | 0.0514 | 0.031 | 0.1764 |
| 384×512×3 | 0.188 | 0.1233 | 0.094 | 0.4053 |
| 227×303×3 | 0.078 | 0.0431 | 0.032 | 0.1531 |
| 300 ×500×3 | 0.078 | 0.0940 | 0.079 | 0.2510 |
| 480×640×3 | 0.157 | 0.1926 | 0.125 | 0.4746 |
| 1500×1200×3 | 0.829 | 1.1285 | 0.671 | 2.6285 |

Table (5): Measurement results components encryption-decryption

| Image size | Encryption time using color image components | Decryption time using gray image |
|---|---|---|
| 256×320×3 | 0.1167 | 0.0814 |
| 227×303×3 | 0.0981 | 0.0731 |
| 300 ×500×3 | 0.2139 | 0.1240 |
| 480×640×3 | 0.4380 | 0.2546 |
| 1500×1200×3 | 2.5659 | 1.7545 |

## 4. Result discussion

From the results obtained in the previous section we can make the following judgment:

1. All the mentioned methods can be used for encryption-decryption purposes without any loss of information.

2. High degree of security, because the size of the matrix key (keys) has varied large and it contains a double number which are hardly predictable.

3. A comparison results are listed in table (4) which shows that the best method to use is R'G'B' because it has a sufficient speedup comparison with the other two methods.

Table (4): Comparison results components

| Image size | Encryp-tion And decryp -tion time using HIS method (1) | Encryp -tion And decryp -tion time using R'G'B' method (2) | Encryption -decryption time using RGB component (3) | Speed up (2) with (1) | Speed up (2) with (3) |
|---|---|---|---|---|---|
| 256×320×3 | 0.3403 | 0.1503 | 0.1981 | 2.2641 | 1.3180 |
| 384×512×3 | 0.7807 | 0.2807 | 0.4355 | 2.7813 | 1.5515 |
| 227×303×3 | 0.2958 | 0.1358 | 0.1712 | 2.1782 | 1.2607 |
| 300 ×500×3 | 0.4793 | 0.2253 | 0.3379 | 2.1274 | 1.4998 |
| 480×640×3 | 0.9026 | 0.4626 | 0.6926 | 1.9511 | 1.4972 |
| 1500×1200×3 | 4.9838 | 3.2358 | 4.3204 | 1.5402 | 1.3352 |

## 5. Conclusions

Different method of color image encryption-decryption were tested and analyzed. The tested methods prove that they are acceptable by means of security and correctness issues. R'G'B' is to be recommended because of the highest performance achieved by this method.

## References

[1] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images,"Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2003, pp. 191-200.

[2] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, Vol. 1, no. 1, 2006, p.127.

[3] H. El-din H. Ahmed, M. K Hamdy, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Optical Engineering, Vol. 45, Issue 10107003, 2006.

[4] B. Mohammad Ali and J. Aman," Image Encryption Using Block-Based Transformation Algorithm," IAENG Int. Journal of Computer Science, Vol. 35, Issue 1, 2008, pp. 15-23.

[5] Li. Shujun, and X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708-711.

[6] B. A. Forouzan, "Traditional Symmetric-Key Ciphers," in Introduction to Cryptography and Network Security, 1st ed., New Yourk, the McGraw-Hill Companies, Inc., 2008, ch. 3, sec. 1, pp. 60-61 [7] Foley, J.D., A. van Dam, S.K.

[7] Feiner and J.F. Hughes, 1990. Computer Graphics, Principles and Practice. 2ndEdn., Addison-Wesley, Reading, ISBN: 0-201- 12110-7: 1174.

[8] Hu, M.P. and X.Y. Ding, 2004. Automated cell13. Hu, M.P. and X.Y. Ding, 2004. Automated cellProceeding of the Intern Conference on ImageProcessing, Oct. 24-27, IEEE Xplore Press, USA., pp: 2737-2740. DOI: 10.1109/ICIP.2004.1421670.

[9] Wyszecki, G. and W.S. Stiles, 2000. Color Science:Concepts and Methods. Quantitive Data and Formulae. 2nd Edn., Wiley, ISBN: 10: 0471399183, pp: 968.

[10] Akram Mustafa and Ziad AlQadi, 2009. Color image reconstruction using a new model. J. Comput. Sci., 5: 250-159.

[11] Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173.

[12] Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A. AbuJazar and Rushdi Abu Zneit Optimized True-Color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, 2010.

**Dr. Ahmed A.M Sharadqh** received his PhD Degree in Computer, computing system and networks from National Technical of Ukraine "Kyiv Polytechnic Institute – Ukraine in 2007. Since 2009, Dr. Ahmed sharadqh has been an assistant professor in the Computer Engineering Department, Faculty of Engineering Technology, at Al-Balqa' Applied University. His research interests include Performance of network ,image processing. FPGA, digital systems design, operating system, and Microprocessors.