A Secure and Accurate Method for RGB Image Encryption

Navneet Dixit[1], Mr. Umesh Kumar Gera[2]
M. Tech Student[1], Asst.Professor[2]
[1,2]Department of computer Science Engineering
[1,2]RAMA University, Kanpur

Abstract- Computerized shading picture is one of the most broadly utilized information type because of different applications. requiring this sort of information, RGB picture may contains important and mystery data, so keeping the picture from being seen by unapproved outsider is an essential errand. Right now will present a novel technique for RGB shading picture encryption-unscrambling; the gave calculation will have the accompanying highlights:Gives a high security level by forestalling the procedure of picture hacking and make it conceivable to comprehend the picture by a non-approved outsider.Gives a high level of precision and here the first picture must match the decoded picture, and the encryption-decoding process must forestall any loss of data or data mutilation.The proposed technique for information encryption-decrypting must be easy to execute, and requires least equipment and programming prerequisites. Must suit ant types of color images with any size or resolution.

Keywords- RGB color picture, key image, PSNR, MSE, speedup, efficiency, throughput.

1. INTRODUCTION

Digital RGB (red, green, blue) color image is a 3D dimensional matrix [1], [2]; each dimension from the three measurements is reserved for a 2D color matrix (Red color, green color and the blue color).

Figure 1 shows an example of RGB color image and the related histograms [3], [4], [5].

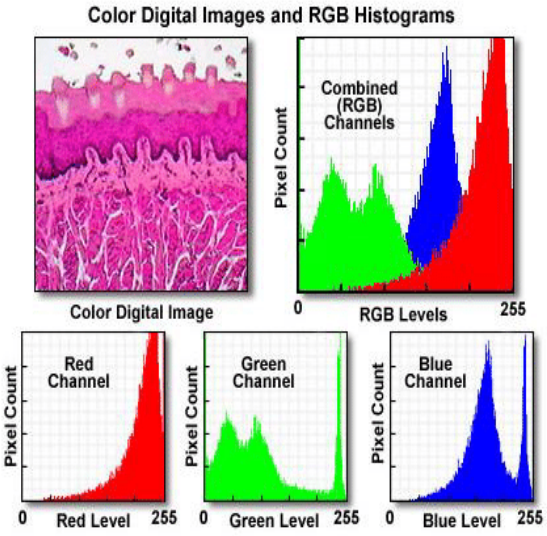

Figure 1 : RGB Color image example and histograms

Each value in a color image ranges from 0 to 255, mixing the three colors together gives the true pixel color as shown in figure 2.

Color name	RGB triplet	Color
Red	(255, 0, 0)	
Lime	(0, 255, 0)	
Blue	(0, 0, 255)	
White	(255, 255, 255)	
Black	(0, 0, 0)	
Gray	(128, 128, 128)	
Fuchsia	(255, 0, 255)	
Yellow	(255, 255, 0)	
Aqua	(0, 255, 255)	
Silver	(192, 192, 192)	
Maroon	(128, 0, 0)	
Olive	(128, 128, 0)	
Green	(0, 128, 0)	
Teal	(0, 128, 128)	
Navy	(0, 0, 128)	
Purple	(128, 0, 128)	

Figure 2 : Mixing the three colors

Real nature is the determination of the color of a pixel on a presentation screen utilizing a 24-bit esteem, which permits the chance of up to 16,777,216 potential hues. ... The quantity of bits used to characterize a pixel's shading conceal is its bit-profundity [31]. Genuine nature is in some cases known as 24-bit color[6], [7].

The quantity of bits used to store every pixel is known as the shading profundity. Pictures with more hues need more pixels to store each accessible shading. This implies pictures that utilization heaps of hues are put away in bigger records [8], [30].

2. COLOR IMAGE ENCRYPTION/ DECRYPTION

The encryption procedure requires a few calculations to scramble the information [29]. Two the figure classes are symmetric and hilter kilter [12]. In symmetric key for encryption, both the sender and beneficiary utilize a similar mystery key and them two knows the key. On the transmitter side, the information is encoded with the mystery key and the beneficiary unscrambles the data with a similar mystery key. The key relies upon the idea of the key. Instances of the fundamental symmetric techniques are the standard for information encryption (DES), Advanced Encryption Standard (AES), universal information encryption calculation (thought). In lopsided key encryption, the two keys utilized are open and private Keys. It has six materials. Making sure about and securing shading picture is an imperative assignment, and it requires [13].

Because of the significance of shading pictures, the proposed encryption-decoding calculation must fulfill the accompanying:

- Provides a high security level by forestalling the procedure of picture hacking and make it
conceivable to comprehend the picture by a non-approved outsider.

- Provides a high level of precision and here the first picture must match the decoded picture, and the encryption-decoding process must forestall any loss of data or data contortion.

- The proposed strategy for information encryption-decoding must be easy to actualize, and requires least equipment and programming necessities.

- Must suit subterranean insect sorts of shading pictures with any size or goals.

Numerous strategies and methods were created for shading picture encryption-decryption[32] [33], a large number of them depend on DES or AES [14], [22], some of them depend on grid augmentation and obstructing by applying xoring utilizing at least one private keys [15-21]. A portion of these techniques have a high level of productivity and worthy degree of security. These strategies utilize a short private key and produce an encoded picture by applying some straightforward math and rationale tasks and here as a result of the short utilized private key it is conceivable to get it and make the scrambled lucid by third unapproved party.

3. THE PROPOSED METHOD OF COLOR IMAGE ENCRYPTION-DECRYPTION

To maintain a strategic distance from the disservices of existing strategies for shading picture encryption-unscrambling, we present another technique which utilizes a unique private key, contemplating the accompanying:
- The private key (mystery key: key picture) is a shading picture.
- Key picture can have any size or goals.
- The sender and the beneficiary must concur on a key picture, and there is no compelling reason to transmit the key picture.
- It is difficult to figure the key since it is inconspicuous.
- The key picture is so colossal, so it is difficult to hack it.
- One key picture can be utilized to encode unscramble various pictures with various sorts and goals.

Figure 3 shows a diagram of the encryption and decryption process:

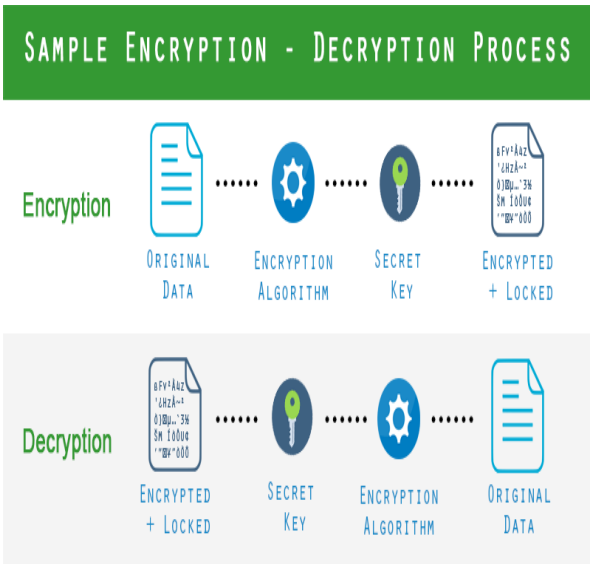

Figure 3 :Diagram of the encryption and decryption process

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed technique was executed utilizing different pictures and different key pictures and the determined pinnacle sign to clamor proportion (PSNR)[23], [24], [25] between the first picture and the unscrambled picture was constantly unending, and furthermore the determined mean square blunder (MSE) between the two pictures was constantly equivalent zero, which implies that the proposed strategy is 100% exact and there no any loss of data during encryption-decoding process usage.

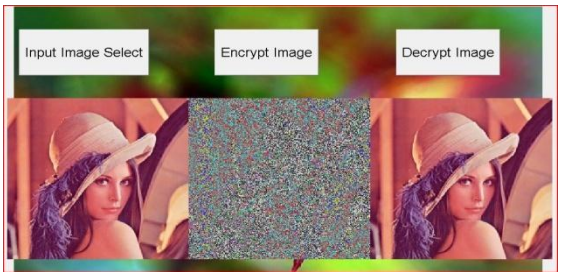

Figure 4 : Implementation Example Outputs

The proposed method was implemented using various images with different size (matlab 7, Intel(R), core™, i5 - 3210M CPU @ 2,5GHz, 4Gbyte RAM, 64 bits OS), table 1 shows the encryption and decryption times:

Table 1: Encryption/decryption time

Key image size = 360x480 x3= 518400 pixels

Image	Resolution	Size (Pixel)	Encryption time(s)	Decryption time(s)
1	152x171 x3	77977	33.518000	0.014000
2	165x247x3	122265	51.887000	0.022000
3	151x 333x3	148059	64.423000	0.027000
4	183x275x3	150975	64.765000	0.028000
5	183x275x3	150975	64.778000	0.028100
6	201x251x3	151353	64.935000	0.035000
7	360x480x3	518400	219.803000	0.134000
8	360x480x3	518400	223.753000	0.129000
9	600x1050x3	1890000	809.791000	0.885000
10	981x1470x3	4326210	1990.797000	2.913000
11	1071x1600x3	5140800	2185.432000	3.744000
Average		**1199800**	**524.8984**	**0.7236**
Pixel time			**0.00043749**	**0.0000006**
Pixel per second			**2285.8**	**1658100**

Here we can see that the relationship between the image size and encryption/decryption time is linear, as show in figures 5 and 6.

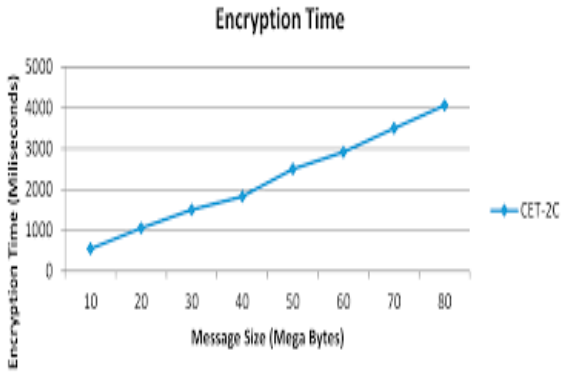

Figure 5 :Encryption time-image size

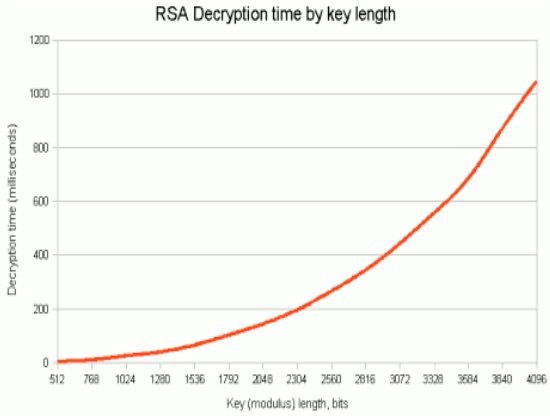

Figure 6 : Decryption time-image size

5. CONCLUSION

An epic technique for shading picture encryption-decoding was proposed, tried and actualized. From the got exploratory outcomes we can raise the accompanying realitieslike :The proposed method can be used to encrypt-decrypt any type of color images with any size and resolution. The secret key is a color image with big variable size, so it is impossible to guess it. The key image is unseen, and there is no need to transmit it.

REFERENCES

[1]. Jamil Al-Azzeh, Bilal Zahran, ZiadAlqadi, BelalAyyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method To Encrypt-Decrypt Color ,International Journal on Informatics Visualization, v. 3, issue 1, pp. 86-93, 2019.

[2]. BelalZahran Rashad J. Rasras, ZiadAlqadi, MutazRasmi Abu Sara, Developing new multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, v. 8, issue 6, pp. 3228-3235, 2019.

[3]. ZiadAlqadi, Bilal Zahran, QazemJaber, BelalAyyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, v. 8, issue 3, pp. 306-319, 2019

[4]. Jamil Al-Azzeh, Bilal Zahran and ZiadAlqadi: Salt and Pepper Noise: Effects and Removal; International Journal on Informatics Visualization July 2018.

[5]. Elamrawy, F., Sharkas, M., and Nasser, A. M., An image encryption based on DNA coding and 2DLogistic chaotic map. International Journal of Signal Processing 3:27–32, 2018

[6]. QazemJaberZiadAlqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.

[7]. Keuninckx, L., Soriano, M. C., Fischer, I., Mirasso, C. R., Nguimdo, R. M., and Vander Sande, G., Encryption key distribution via chaos synchronization. Scientific Reports:1–14, 2017

[8]. Dr. Ziad A. AlQadi, Dr. Hussein M. Elsayyed, Window Averaging Method to Create a Feature Victor for RGB Color Image, IJCSMC, Vol. 6, Issue. 2, February 2017, pp. 60 – 66

[9]. Usama, M., and Zakaria, N., Chaos-based simultaneous compression and encryption for Hadoop. PLoS ONE 12(1):1–29, 2017

[10]. Khare, A., Shukla, P. K., Rizvi,M. A., and Stalin, S., An intelligent and fast chaotic encryption using digital logic circuits for ad-hoc and ubiquitous computing. Entropy, MDPI 18(201):1–27, 2016

[11]. Mondal, B., and Mandal, T., A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University, Computer and Information Sciences:1–6, 2016
[12]. Liu, L., and Miao, S., A new image encryption algorithm based on logistic chaotic map with varying parameter. Springer Plus 5(289): 1–12, 2016
[13]. Shukla, P. K., Khare, A., Rizvi, M. A., Stalin, S., and Kumar, S., Applied cryptography using Chaos function for fast digital logicbased Systems in Ubiquitous Computing. Entropy, MDPI 17:1387 1410, 2015.
[14]. Huang, X., Sun, T., Li, Y., and Liang, J., A color image encryption algorithm based on a fractional-order Hyperchaotic system. Entropy, MDPI 17:28–38, 2015
[15]. Tong, X., Yang, L., Zhang, M., Xu, H., and Zhu, W., An image encryption scheme based on Hyperchaotic Ra, binovich and exponential Chaos maps. Entropy,MDPI 17:181–196, 2015
[16]. Soleymani, A., Nordin,M. J., and Sundararajan, E., A chaotic cryptosystem for images based on Henon and Arnold cat map. The scientific world journal, Hindawi:1–21, 2014
[17]. Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi , Analysis of Matrix Multiplication Computational Methods European Journal of Scientific Research Vol.121 No.3, 2014, pp.258-266
[18]. Haitham A. Alasha'ary, Khaled M. Matrouk, Abdullah I. Al-Hasanat, Ziad A. Alqadi, Hasan M. Al-Shalabi, Improving Matrix Multiplication Using Parallel Computing, *International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6, ISSN 2281-2911 November 2013*.
[19]. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abu jazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, v. 8, issue 10, pp. 1175-1182, 2010.
[20]. A Waheeb, ZiadAlQadi, Gray image reconstruction, Eur. J. Sci. Res, v. 27, pp. 167-173, 2009