I.J. Image, Graphics and Signal Processing, **2016, 7, 67-72**
Published Online July 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.07.08

A Secure Algorithm for Region of Interest (ROI) Encryption for RGB Color Images

Aniruddha G. Phatak
Department of Electronics and Telecommunications, PVG's College of Engineering and Technology, Pune, India.
E-mail: aniruddhaphatak93@hotmail.com

Abstract—An algorithm optimized towards encrypting a specific region in an image is proposed. The encryption of specific region(s) in an image is often of more practical relevance than encrypting the entire image, thus avoiding wastage of time and processing power. The algorithm proposed is ideal for encrypting images with relatively small Region of Interest (ROI). It makes novel use of the XOR operation and the relative visual redundancy of the blue-plane components in a RGB color image. A pseudorandom number generator is used as a basic security feature. Furthermore, Cipher Block Chaining (CBC) is also suggested as an improvement to further enhance the security of the algorithm. The algorithm may be classified as lossy since some visual data is sacrificed in the decrypting process. However, in case of encryption algorithms, the high security of the encrypted image is often given priority over faithful reproduction of images.

Index Terms—Image encryption, Region of Interest, XOR, Pseudorandom generator, Cipher Block Chaining.

I. Related Work

It is trivial to prove that the set of all numbers of bit length n form a finite group under the operation XOR with the order of the group being 2^n. Given the result of an XOR operation, it requires us to brute force through the entire 2^n elements and their combinations and yet the result will not be unique. It is easy to show that given the result of m elements of n bits XORed together, there are $\mathbf{2^{(n)(m-1)}}$ possible combinations that will yield the same result. The algorithm makes use of this concept.

Most digital image encryption algorithms are based on the concept of chaotic maps. Chaos theory was first proposed as a cryptographic tool by Robert Matthews [1] in 1989. There are several classes of chaos functions, of which the logistics map is the simplest and the most widely used (MS Baptista [2]). Thereafter there have been several publications relating to the same, most notably by Guan, Guan and Huang [3]. Shuffling and scrambling of pixels values based on chaotic maps have been the basic skeleton of all related algorithms. Chen, Mao and Chui [4] and Pareek, Patidar and Sud [5] are other notable mentions. Another algorithm that vaguely resembles the one proposed in this paper in due to Jui Cheng [7] in which a VLSI based algorithm is proposed which is based on XORing and XNORing the value each pixel in a grayscale image with predetermined keys, determined according to a chaotic binary sequence. The XOR operation is also used in the proposed algorithm.

However chaotic image encryption has its drawbacks. Jakimoski and Kocarev [6] carried out a detailed critical of these systems and several of them rely on the assumption that the attacker does not know the chaotic function or the chaotic map used. This assumption is contradictory to the basic tenet of modern cryptography, known as the Kerchoff's principle [8], which states that the security of the algorithm should only be guaranteed by the secret key and never by the algorithm itself.

Some other approaches proposed in literature include that of optical image encryption using fractional Fourier transforms notably by Refregier and Javidi [9] and Hellenley and Sheridan [10]. Other notable approaches include that due to Loukhoukha, Chouinard and Berdai [11] which is based on the principle of Rubiks Cube. The method was shown to have appreciable resistance to brute force attack. In the same paper the authors also pointed out several drawbacks of the popular chaotic map methods, one of the more important ones being the use of relatively small key spaces.

Many image encryption algorithms also employ the principle of cipher block chaining, a variation of which is used in this paper, in which the cipher text of the previous cipher block is XORed with the next plaintext before it is encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point (Bellare, Killian and Rogaway [12]). In case of images the individual cipher blocks are the individual pixels.

The principle of pseudorandom number generation is central to the modern cryptography. There are numerous PRNGs described in literature, based on number theory or hash functions. One of the landmark PRNG algorithms was described by Blum, Blum and Shub [13]. PRNG's add the necessary controlled randomization to a system by generating periodically repeating random binary sequences. However, because of the extremely large sequences which depends on the seed length (if the seed length is N, then the maximum period of the binary sequence is $2^N - 1$), the binary sequence appears random.

II. Algorithm Description

In this section, the encryption and decryption algorithm is described in detail.

Copyright © 2016 MECS

A. Encryption Algorithm Description

Let the overall dimension of the image be m x n and the dimension of the region to be masked be p x q. this region is henceforth referred to as 'region of interest' (ROI).

1. Each pixel in the image is numbered in the Raster format (left to right and top to bottom) from 1 to m×n, where m×n is the dimension of the entire image.
2. A seed of x number of bits is given as input from the true RNG to the pseudo RNG. The pseudo RNG generates a bit stream of length

$$L = p \times q \times \log2\ (m \times n) \text{ bits} \quad (1)$$

3. The input to the PRNG (Pseudorandom number generator) is of length x given as

$$x = \log2\ (L) = \log2\ (p \times q \times \log2\ (m \times n)) \text{ bits} \quad (2)$$

4. The PRNG bit stream is divided into p×q chunks of length log2 (m×n).
5. Each chunk represents a pixel location which lies outside the region of interest as per the numbering done in the Raster format. If any chunk refers to a location inside the ROI, then another stream of length log2 (m×n) is demanded from the PRNG. Note that smaller the ROI, lesser will be the retransmission demands by the encrypter to the PRNG.
6. Each chunk is assigned to each pixel in the region of interest. As mentioned above each chunk is a pointer to a pixel *outside* the ROI.
7. To encrypt the first pixel in the ROI (say A):

The 8- bit data from the three RGB planes is processed ad follows: Each plane is required to have exactly 8 bits. The R and the G planes are added leading zeros if their length is less than 8 bits. The B plane is added *trailing* zeros if its length is less than 8 bits.

The three 8-bit values are concatenated as follows:

$$T = \text{concat}\ (B, G, R) \quad (3)$$

where concat represents concatenation.

Let P(1) represent the PRNG stream assigned to pixel 1. Let the pixel value at the location P(1) be Z(1).

8. Let R(1) be given as:

$$R(1) = \text{bitXOR}\ (\ T(1), Z(1)\ ) \quad (4)$$

Note that R(1) is invariably of 24 bits since T(1) is invariably of 24 bits.

9. Now the encrypted value of the pixel A is simply

$$E(1) = \text{bitXOR}\ (\ R(1), P(1)\ ) \quad (5)$$

where bitXOR is the bitwise-Exclusive OR operator.

10. Similarly repeat for all the other pixels in the ROI, A(i) where i = 1 to p×q.

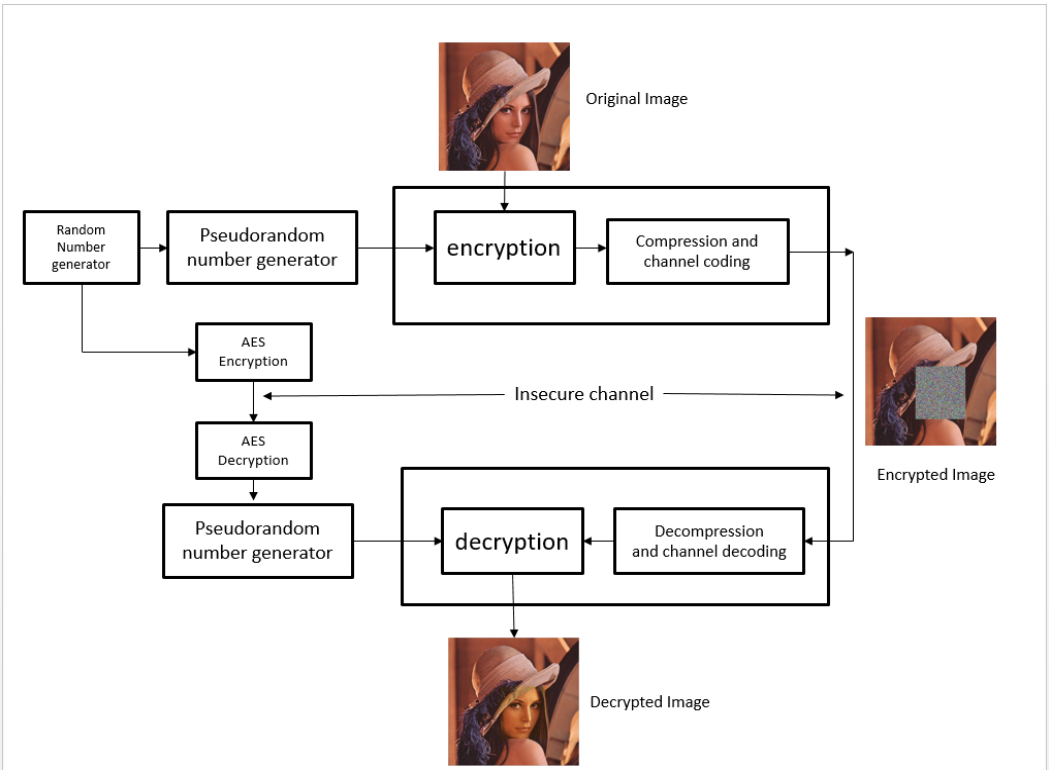


Fig.1. Block Diagram of the Encryption and the Decryption Algorithm

Copyright © 2016 MECS

B. Decryption Algorithm Description

1. The decoding process is quite straightforward. Since XOR is a reversible operation, XORing E(i) with P(i) will lead to the result R(i).
2. Note that the PRNG bit stream needs to be exactly replicated at the receiver. For this the seed is securely transmitted to the receiver using the standard cryptographic algorithms such as RSA and DES.
3. Once P(i) is obtained it is a trivial process to obtain A(i) using the value of Z(i) as pointed to by the value P(i), in the following manner:
4. Consider the first pixel in the ROI. The received code word E(1) is bitXORed with the value of the PRNG stream assigned to pixel 1 i.e. P(1). This process will yield R(1) = bitXOR (T(1), Z(1)).
5. As Z(1) is a pixel which is outside the ROI and is hence, unencrypted, its value is available to the decoder. The decoder uses this value of Z(1) to calculate the value of T(1) by again applying the XOR process.
6. Once T(1) is evaluated, it is divided into three chunks of 8 bits each. (T(1) is invariably of 24 bit length). The first chunk from the left is the B-plane value which has trailing zeros appended to make its length equal to 8 bits.
7. All the leading zeros are removed from this value. Note that this will lead to losing of the LSB bits in cases where there were one of more trailing zeros prior to the appending of the extra zeros. The B-plane was selected since this plane contributes the least to the visual information contained in the image. One of the two other planes could also have been chosen, leading to an image with much lesser fidelity, as can be seen in the images in the next section. As such, this process does not reproduce the image with 100% fidelity, but the fidelity is more than sufficient in most practical applications.
8. The other two chunks are part of the G-plane and the R-plane. These planes have leading zeros appended. Obviously, their removal does not lead to losing any data as in the case of the B-plane. Hence the red and the green components of a pixel, which contribute the most visual information, are reproduced perfectly.
9. Finally, the decoded RGB planes are combined to obtain the original unencrypted portion of the image.

III. Improvements

In this section, cipher block chaining is suggested as a method that can be used to improve the security of the algorithm.

A. Cipher Block Chaining

The concept of CBC was invented by IBM in 1976. Each encrypted block of data of the previous pixel are combined through the XOR operation with the current pixel data before encryption. This makes the encrypted output of the current block depend not only on the current pixel data but also on the data of all the previous pixels. Hence any error in calculating a pixel value propagates through the entire image block in increasing magnitude; a pixel only a small distance away from the current pixel will become too scrambled due to such error propagation to convey the original information faithfully. CBC tremendously increase the security of a block cipher system as will be shown in the analysis section.

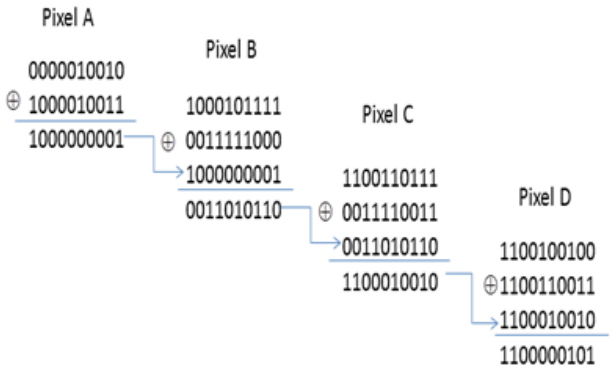


Fig.2. Cipher Block Chaining

IV. Security Analysis

A. Brute Force Attack

If m numbers each of n bits are combined together through the XOR operation as shown below, the total number of combinations that yield the same answer is $2^{(n)(m-1)}$.

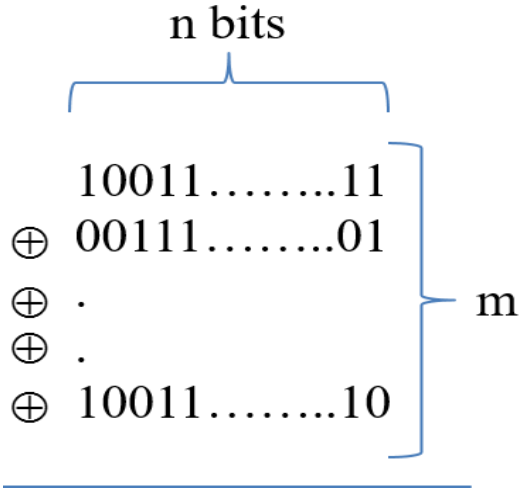


Fig.3. XORing of m Numbers Each of N Bits

Using the same principle, an encryption of a p × q ROI (and considering the use of CBC), the number of combinations to brute force the algorithm would be (since we are only considering PRNG values that are outside the ROI):

$$2^{(24)} \times 2^{(3)(24)} \times 2^{(5)(24)} \times 2^{(7)(24)} \text{.....(m-p)} \times \text{(n-q) times} = 2^{(24)(1+3+5+7\ldots.(m-p)(n-q)\ \text{elements}} \quad (6)$$

Applying the formula of simple arithmetic progression, we have

$$2^{24(m-p)2(n-q)2} \quad (7)$$

possible combinations for a 24-bit RGB image with a ROI of p x q dimension and m x n total dimension.

Hence a brute force attack on the algorithm will consume huge time and computing power since the number of possible combinations that would have to be implemented would be extremely large.

From the formula, it is obvious that a small ROI offers larger security. Such a small ROI is also advantageous in minimizing the retransmission requests from the encrypter to the PRNG, since the encrypter will request retransmission each time the input pseudo random bit stream points to a pixel inside the ROI.

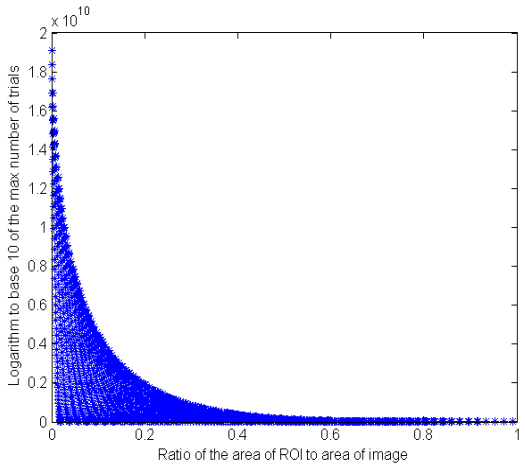


Fig.4. Plot of the base 10 logarithm of the maximum number of trials required to brute force the algorithm versus the ratio of the area of the ROI to the area of the image. Note the exponential decrease in the number of trials required to brute force as the area of the ROI increases (i.e. ratio on the x-axis increases.) Also note the huge number of trials required for a large ROI.

V. Selection of the B-Plane

It is well established that blue light contributes the least to the visual perception of humans compared to green (largest) and red (average). This fact is also reflected in the formula of the luminance component is the YCbCr color space as:

$$Y = 0.2126\ R + 0.7152\ G + 0.0722\ B \quad (8)$$

One of the three 8 –bit RGB values is required to have a non-zero starting bit (and hence no leading zeros), so that the combination of all three RGB values invariably yields a 24-bit number. The decoding of a value that has trailing zeros will lead to losing of the rightmost (LSB) zeros, if any, since the decoder discards all trialing zeros irrespective of their origin. The B-plane is selected to carry the trailing zeros instead of the leading zeros precisely for this reason, since data loss of the blue component while decoding is much more acceptable that the green and the red component. Hence the value of T in the algorithm described above has the leftmost component as blue instead of the conventional red in the RGB system.

Note that the images decrypted in this manner will be lossy but in the case of encryption algorithms, high security of the encrypted image is often of higher priority than faithful reproduction of the image.

VI. Results

In this section, several applications and hypotheses are demonstrated. In section (A), the the algorithm is applied for the purpose of facial masking. In Section (B), a hypothetical situation is presented in which the ROI is equal to the area of the entire image. In the third sub-section, the R and G-pixel components are chosen to bear data loss (se Section V). Finally in the last section, an example of a larger ROI is demonstrated.

A. Facial Masking

The object masking or region masking algorithm can also be specifically used for facial masking for withholding the identity of a person. This algorithm is ideal for facial masking since in general, the area of the face of a person is an image is small compared to the overall area of the image. As is explained in the previous sections and illustrated in Fig 4, this algorithm is ideal for encrypting small Regions of Interests (ROI), since larger ROI would imply more ‘retransmission requests’ from the encrypter to the PRNG. Another application that is similar to facial masking is that of number plate masking.

In the below result images, facial masking using the proposed algorithm is shown. In Fig 5 (c), the decrypted image is shown. The yellowish hue seen in the decrypted ROI is because of the discarding of the trailing zeros of blue-plane pixels by the decoder. This leads to increased relative intensity of Red (R) and Green (G) components of the pixels, which when combined results in the yellowish hue. As in mentioned in the previous sections, the algorithm is lossy in nature. However, in most encryption systems, higher security has higher priority over exact faithful reproduction of the original image.

(a) (b)

Copyright © 2016 MECS

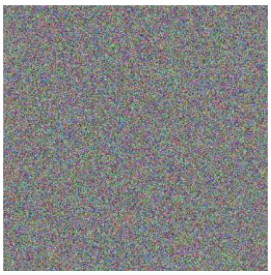
(c)

Fig.5. (a) Original Lenna test Image (b) Encrypted Image with ROI-masking (c) Decrypted image. Note the yellow hue in the decrypted ROI region due to the loss of blue-component data caused by the discarding of trailing zeros by the decoder. The region appears yellowish due to increased relative intensity of the red and green components.

B. Hypothetical situation in which ROI is the entire image (p = m and q = n)

In this sub-section, a hypothetical situation is presented in which the ROI is the entire image. As can be seen in Fig 6 (c), the yellowish hue now covers the entire image. This situation is practically impossible since the input of the PRNG must be a pointer to a pixel in the non-ROI area (otherwise there is a retransmission request from the encrypter) – since there is no non-ROI area in this case, every input from the PRNG will entail a retransmission request.

(a)



(b)

(c)

Fig.6. (a) – (c) Hypothetical situation when p = m and q = n. Original, encrypted and decrypted image. Again note the yellow hue in the entire decrypted image. Such encryption of large sections image by arbitrarily increasing value of p and q is not practical since it would lead to huge number of retransmission requests to the PRNG. In this case, for encrypting the entire image, every input from the PRNG would have a return retransmission request from the encrypter.

C. Scenarios in which R and G plane components are selected to incur data loss

In this sub-section, the Red (R) and the Green (G) pixel components are selected to bear information loss instead of the Blue (B) component. Fig 7 (a) is the original image and Fig 7 (b) and Fig 7 (c) represent scenarios in which the R and the G components bear data loss. Note the lower amount of fidelity compared to Fig 6 (c).

(a)

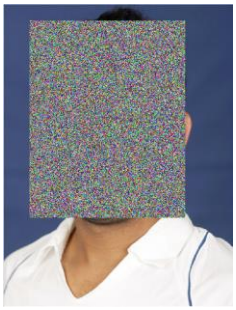
(b)

(c)

Fig.7. (a) – (c): Original image and images in which the R-plane components and the G-plane components are used to append trailing zeros respectively, instead of the blue plane components. Note the relatively larger fidelity loss than in fig 6(c).

D. Example of larger ROI

(a)



(b)

(c)

Fig.8 (a) – (c): Example in which the ROI is large compared to the original dimensions of image. In such a scenario, the numbers of retransmission requests to the PRNG are much larger, leading to consumption of large processing power and lower encryption speed. Also the effect of data loss during decryption is spread over a larger area causing distinctly poor image fidelity.

Copyright © 2016 MECS

In this last sub-section, an example in which the ROI is quite large compared to the image is given. Such a large ROI is not ideal and will lead to large number of retransmission requests. Also, note the poorer image fidelity in Fig 8 (c) compared to Fig 5 (c). This is due to the relatively larger ROI compared to Figure set 5.

VII. Conclusion

In this paper, a novel algorithm for ROI-masking and encryption was proposed. The algorithm is lossy and is optimized for relatively smaller ROI compared to the image dimension. For larger ROI, it leads to slower speeds and distinctly poorer image reproduction.

References

[1] Robert Matthews, "On the derivation of a 'chaotic' encryption algorithm", Cryptographia, Volume 13, Issue 1, 1989.
[2] MS Baptista, "Cryptography with chaos", Elsevier, 1998.
[3] Zhi-Hong Guan, Wenjie Guan and Fangjun Huang, "Chaos based image encryption algorithm", Elsevier, October 2005.
[4] G Chen, Y Mao, CK Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Elsevier, 2004.
[5] NK Pareek, V Patidar, KK Sud, "Image encryption using chaotic logistic map", Elsevier, 2006.
[6] L Kocarev, G Jakimoski "Logistic map as a block encryption algorithm", Physical letters, Elsevier, 2001.
[7] Jui Cheng, "A new chaotic key-based design for image encryption and decryption ", IEEE Circuits and Systems, 2000.
[8] Auguste Kerckhoffs, "La cryptographie militaire" *Journal des sciences militaires*, vol. IX, pp. 5–83, January 1883.
[9] Phillipe Refregier and Bahram Javidi," Optical image encryption using input plane and Fourier plane random encoding", SPIE, 1998.
[10] B Hennelly, JT Sheridan, "Optical image encryption by random shifting in fractional Fourier domains", Optics Letters, 2003.
[11] Khaled Loukhaoukha, Jean-Yves Chouinard, Abdellah Berdai, "A Secure Image Encryption Algorithm Based on the Rubik's Cube Principle", Journal of Electrical and Computer Engineering, 2012.
[12] M Bellare, J Killian, P Rogaway, "The security of cipher block chaining", CRYPTO'94 Journal, 1994.
[13] L Blum, M Blum, M Shub, "A simple Unpredictable Pseudo-random Number generator", SIAM Journal of Computing, 1986.

Authors' Profiles

Aniruddha Phatak is a graduate in Electronics and Telecommunication Engineering from the University of Pune. Currently, he is working as a research intern at the Centre of Excellence in Signal and Image Processing at the College of Engineering Pune, and plans to pursue further research opportunities in signal and image processing in the United States. His research interests include digital signal, image and video processing, cryptography and information theory.

How to cite this paper: Aniruddha G. Phatak,"A Secure Algorithm for Region of Interest (ROI) Encryption for RGB Color Images", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.7, pp.67-72, 2016.DOI: 10.5815/ijigsp.2016.07.08

Copyright © 2016 MECS