Image Encryption Algorithms Based on Generalized P-Gray Code Bit Plane Decomposition

Yicong Zhou, *Member, IEEE*, Karen Panetta, *Fellow, IEEE*, and Sos Agaian, *Senior Member, IEEE*

***Abstract*—Image encryption is an effective method to protect multimedia information for different security purposes. In this paper, we introduce a new image bit-plane decomposition method based on the Generalized P-Gray Code (GPGC) which is a parametric sequence suitable for any base, n. Based on this decomposition, we introduce two image encryption algorithms using GPGC. The two algorithms allow for either full or partial encryption of images based on the choice of security keys: base n and distance parameter p. Experimental results show that the presented algorithms are lossless encryption methods, and that the original images can be completely reconstructed when the correct security keys are used. It is also shown that the presented algorithms can withstand the plaintext attacks.**

***Index Terms*—Image Encryption, Generalized P-Gray Code, bit plane decomposition, P-Gray Code decomposition**

I. Introduction

UBIQUITOUS network and computer technologies have provided great flexibility and opportunities for people all over the world to store, transmit and share multimedia information. As a result, the security of images and videos becomes a prevalent issue not only for individuals and business but also for government and the military. Image encryption is an effective and well-known method to protect images and videos by transforming them into unrecognizable formats. Image encryption is widely used in different application areas such as privacy and copyright protection, security communication, and military applications as well.

Several encryption methods have been developed to encrypt images recently such as image encryption based on chaotic sequence [1, 2], Fibonacci sequence [3], and Gray Code [4]. These approaches don't have enough security keys to achieve higher security levels. We presented an image encryption method based on Generalized P-Gray Code (GPGC) in our previous work which introduced more security keys [5]. However, these permutation-only based encryption methods cannot tolerate plaintext attacks [6].

Some interesting image encryption schemes are based on binary bit plane decomposition [7-9]. Bit plane decomposition is a process to decompose the grayscale image into n binary images called n bit planes. The order of the bit planes is from the most significant bit to the least significant bit. Each bit plane consists of all binary bits with the same order in the n-bit binary sequences of all pixels. However, this type of decomposition process has low security level since it is not parameter-dependent.

In this paper, we introduce a new parameter-dependent bit-plane decomposition scheme based on Generalized P-Gray Code (GPGC) and two GPGC decomposition based image encryption algorithms. There are many options for the base n and parameter p of GPGC as security keys for GPGC decomposition process and encryption process. The encrypted images are difficult to be broken without correct security keys. The presented algorithms can resist the plaintext attacks since the process of the GPGC bit plane decomposition changes image pixel values. The experimental results show that the presented algorithms can partially or fully encrypt images based on different n and p values such that images can be protected with different security levels to meet different security requirements.

The rest of this paper is organized as follows. GPGC decomposition will be introduced in section 2. Section 3 will address the image encryption algorithms. Experimental results are shown in section 4. Security issues will be discussed in section 5. Section 6 presents a concluding discussion.

II. Generalized P-Gray Code Decomposition

In this section, we extend the conception of bit plane representation of grayscale images from binary to arbitrary base for image encryption purposes. We introduce a new bit plane representation of grayscale images using Generalized P-Gray Code.

Definition 2.1: *Arbitrary-base bit plane decomposition*

Let an $M \times N$ image be represented by a k-digit n-base sequence $(a_k a_{k-1} \cdots a_2 a_1)_n$, the grayscale image can be decomposed into k arbitrary-base bit planes. The pixel value

Yicong Zhou and Karen Panetta are with Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155 USA (YZ phone:1-617-627-5183;fax:1-617-627-3220; e-mail: yzhou0a@ece.tufts.edu; KP e-mail: karen@ece.tufts.edu).

Sos Agaian is with Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA (e-mail: Sos.Agaian@utsa.edu).

in the i^{th} bit plane is the i^{th} bit a_i of the pixel with the same location in grayscale image, where $1 \le i \le k$.

Definition 2.2: *Generalized P-Gray Code* [5]

If $(a_k a_{k-1} \cdots a_2 a_1)_n$ is the k-digit n-base representation of the non-negative integer A, assume a k-digit n-base sequence $G = (g_k g_{k-1} \cdots g_2 g_1)_n$ is satisfied with

$$g_i = \begin{cases} a_i & i > k - p - 1 \\ (a_i + a_{i+p+1}) \bmod n & 1 \le i \le k - p - 1 \end{cases} \quad (1)$$

where $1 \le i \le k$ and $0 \le p \le k$, G is the Generalized P-Gray Code (GPGC) of A. It also called *(n, k, p)*-Gray Code representation of A.

The GPGC will be different based on the different values of *n* and *p*. For example,

1) For *n=2*, the GPGC is the binary P-Gray Code;
2) For *n=2*, *p=0*, the GPGC reverts to the classical gray code;
3) For *n=3*, the GPGC is the ternary P-Gray Code;
4) If n is other value, the GPGC will be different P-Gray Code.

Definition 2.3: *Generalized P-Gray Code decomposition*

If each pixel value in a grayscale image can be represented by a k-digit n-base sequence $(a_k a_{k-1} \cdots a_2 a_1)_n$, and it GPGC representation is the sequence $(g_k g_{k-1} \cdots g_2 g_1)_n$ based on definition 2.2, the grayscale image can be decomposed into k GPGC bit planes, where the pixel value in the i^{th} plane is the i^{th} bit g_i of the pixel with the same location in grayscale image,

where $1 \le i \le k$.

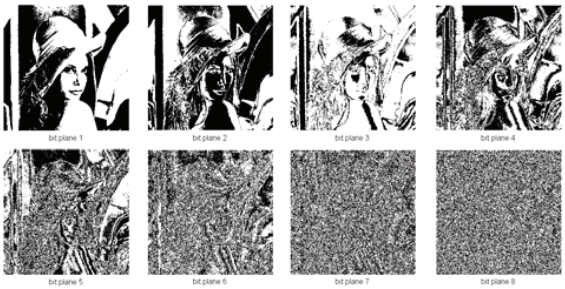

Fig. 1. GPGC bit plane decomposition of the grayscale image, *n=2, p=1*

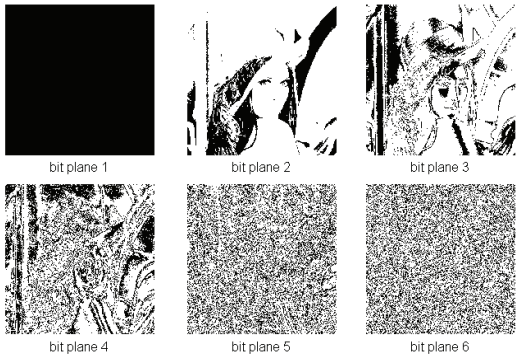

Fig. 2. GPGC bit plane decomposition of the grayscale image, *n=3, p=1*

The GPGC bit planes will differ according to different base *n* and parameter *p*. The number of GPGC bit planes will change with different *n* value. A grayscale image can be decomposed to 8 binary bit planes when base *n=2*. An example is shown in Fig. 1 with *n=2, p=1*.

When the base *n* is greater than 2, the decomposed bit planes of a grayscale image will not be binary any more and the number of bit planes will be less than 8. An example is shown in Fig. 2 with *n=3, p=1*.

III. GPGC Transforms and Image Encryption Algorithms

In this section, we review several GPGC transforms which were presented in our previous work [5]. We will introduce two new image encryption algorithms based on GPGC decomposition and GPGC transforms. One algorithm is for grayscale image encryption. The other works for color image encryption.

A. Generalized P-Gray Code Transforms [5]

Definition 3.1: For a non-negative integer sequence $A = \{A_1, A_2, A_3, ..., A_m\}$, the following transformation is called the 1-D Generalized P-Gray Code Transform. The integer sequence $G = \{G_1, G_2, G_3, ..., G_m\}$ is the GPGC representation of A.

$$G = (C_p * A) \bmod n \quad (2)$$

where

$$G = \begin{pmatrix} G_1 & G_2 & \dots & G_m \end{pmatrix}_{10} = \begin{pmatrix} g_{11} & g_{21} & \cdots & g_{m1} \\ g_{12} & g_{22} & \cdots & g_{m2} \\ \dots & \dots & \dots & \dots \\ g_{1k} & g_{2k} & \cdots & g_{mk} \end{pmatrix}_n$$

$$A = \begin{pmatrix} A_1 & A_2 & \dots & A_m \end{pmatrix}_{10} = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \dots & \dots & \dots & \dots \\ a_{1k} & a_{2k} & \dots & a_{mk} \end{pmatrix}_n$$

and $C_p = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1k} \\ c_{21} & c_{22} & \dots & c_{2k} \\ \dots & \dots & \dots & \dots \\ c_{k1} & c_{k2} & \dots & c_{kk} \end{pmatrix}_p$

where

$$\left(c_{ij}\right)_p = \begin{cases} 1 & i = j \\ 1 & j = i + p + 1, i + p + 1 \le k \\ 0 & otherwise \end{cases}$$

k, m, n and *p* are non-negative integer, $1 \le i, j \le k$, $0 \le p \le k$.

Using the above transform, when the base *n* and parameter *p* have different values, an input sequence $(1,2,3,...,N)$ can be transferred to different permutation sequences,

$$G_p = (G_1, G_2, G_3, ..., G_m)_p \quad (3)$$

Specially, when input sequence has only one integer element, $A = \{A_1\}$ for example, the transform definition above will be another format of GPGC in definition 2.2.

$$\begin{pmatrix} g_{11} \\ g_{12} \\ \dots \\ g_{1k} \end{pmatrix} = (C_p \begin{pmatrix} a_{11} \\ a_{12} \\ \dots \\ a_{1k} \end{pmatrix}) \bmod n \quad (4)$$

To recover the original integer sequence, we can use the inverse 1-D GPGC transformation which is defined below.

Definition 3.2: If the sequence $\{G_1, G_2, G_3, ..., G_m\}$ is the Generalized P-Gray Code representation of the sequence $\{A_1, A_2, A_3, ..., A_m\}$, the following transformation is called the Inverse 1-D GPGC Transform.

$$A = (C_p^{-1} * G) \bmod n \quad (5)$$

where A, G, C_p and m, n, p, k are given by definition 2.2.

The 1-D GPGC transform can be used to encrypt one dimensional media data such as a string, password, audio or speech signals. It can be also used to encrypt 2D images line by line, for example medical images. However, its encryption process is time-consuming.

Definition 3.3: Let D be an $M \times N$ image, T_r and T_c be the row and column coefficient matrices respectively, the 2-D GPGC Transform is defined as:

$$E = T_r D T_c \quad (6)$$

where E is the encrypted 2-D image and,

$$T_r(m,n) = \begin{cases} 1 & (m, G_{pm}) \\ 0 & otherwise \end{cases} \quad T_c(i,j) = \begin{cases} 1 & (G_{pj}, j) \\ 0 & otherwise \end{cases}$$

where $1 \le m, n \le M$, $1 \le i, j \le N$, G_p is a permutation sequence defined by equation (3).

Definition 3.4: Let E be the encrypted 2-D images, T_r and T_c be the row and column coefficient matrices respectively, the following transformation is called Inverse 2-D GPGC Transform.

$$R = T_r^{-1} E T_c^{-1} \quad (7)$$

where R is the reconstructed image matrix.

The 2-D GPGC transform is a more efficient process to encrypt 2D images than the 1-D GPGC transform because it can encrypt 2-D images by applying the 2-D GPGC transform only one time. Furthermore, to reconstruct the original 2D image, we simply apply the 2-D inverse transform one time.

B. Grayscale Image Encryption Algorithm

Fig. 3 shows the encryption algorithm of grayscale image. The grayscale image is decomposed into GPGC bit planes. The 2-D GPGC transform can encrypt these GPGC bit planes one by one. The encrypted GPGC planes are converted to decimal pixel value to obtain the encrypted grayscale image.

To encrypt the grayscale image, the security keys, base n and parameter p, should be selected first. The user has flexibility to choose same or different security keys for image decomposition and encryption processes. When base n and parameter p are different, the GPGC bit planes of images will be different and the row and column coefficient matrices of GPGC transform are also different.

The decryption algorithm shown in Fig. 4 is an inverse process of encryption algorithm. To reconstruct the original image, the authorized users should have the security keys: base n and parameter p. The security keys are used to reconstruct the GPGC bit planes and also the row and column coefficient matrices for the inverse GPGC transforms as well.

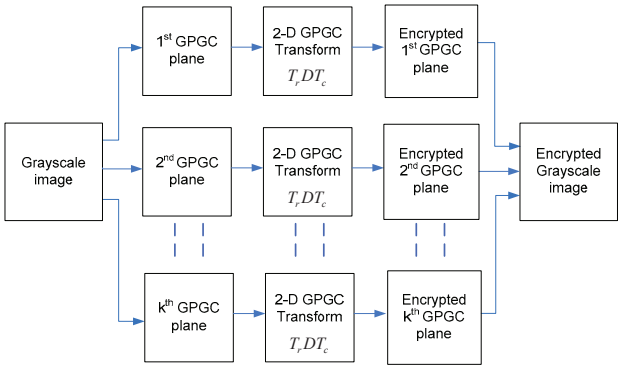

Fig. 3. Block diagram of the grayscale image encryption algorithm

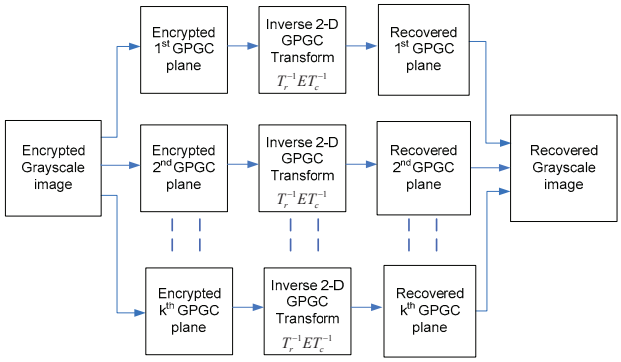

Fig. 4. Block diagram of the grayscale image decryption algorithm

C. Color Image Encryption Algorithm

The color images have three color planes. The data for each color plane is a 2-D data matrix which is similar to grayscale images. Therefore, we consider each color plane as a grayscale image.

The color images encryption is also based on the GPGC decomposition and the 2D GPGC transform. The color image is separated into three color planes which are three 2D data matrices. Each color plane will be encrypted individually by using the same process as the grayscale image encryption. The encrypted color image can be obtained by combining the three encrypted color planes.

The users can choose the same security keys (base n and parameter p) for decomposition and encryption processes of three color planes. They can also choose different keys for each process and also each color plane.

In color image decryption process, the authorized users separate the encrypted color images into three color planes. The correct security keys are used for GPGC decomposition and decryption process of each color plane. The decryption process for each color plane is the same process as the decryption of grayscale image. The three recovered color planes are combined to get the recovered color image.

IV. Experimental Results

We present and discuss the experimental results of grayscale image encryption and color image encryption in this section.

A. Grayscale Image Encryption

Fig. 5 shows an example of the grayscale image encryption with security keys: *n=2, p=2* for GPGC decomposition process and *n=3, p=1* for encryption process. The original image can be perfectly reconstructed. This can be verified from the reconstructed image (Fig. 5(b)) and the histogram of the difference between the reconstructed image and the original image (Fig. 5(c)).

Fig. 5. Grayscale image Encryption with *n=2, p=2* for GPGC decomposition and *n=3, p=1* for encryption. (a) Encrypted image; (b) Reconstructed image; (c) Histogram of the difference between reconstructed grayscale image and original grayscale image.

More encryption examples are provided with *n=3, p=1* for GPGC decomposition and different *n* and *p* value for encryption process in Fig. 6. The encryption results with higher *p* values are more recognizable than the results where *p* has lower value. The better encryption results are obtained where *p* has a smaller value. This is because for smaller value of *p*, the number of image pixel permutations in encryption process increases.

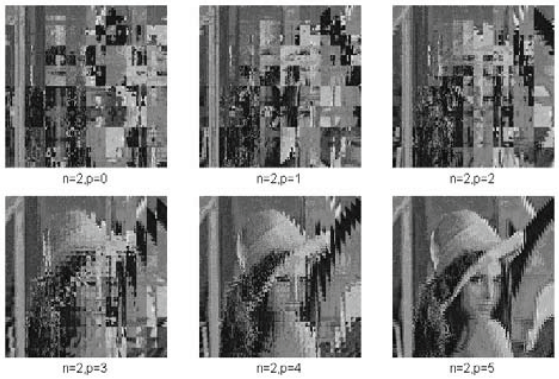

Fig. 6. Grayscale image Encryption with n=3, p=1 for GPGC decomposition and different n and p value for encryption.

Similarly, the percentage of image encryption also decreases if base *n* goes higher. The digital sequence representation will be shorter when base *n* increases. The result is the same as that of higher *p* value. This shows that presented algorithms can encrypt images with different security levels.

B. Color Image Encryption

Color images can be encrypted by decomposing each color plane into GPGC bit planes and then using 2D GPGC transform to encrypt each GPGC plane. The users have the flexibility to use the same security keys for both decomposition and encryption process of all color planes (Fig. 7) or choosing different *p* and *n* values for each color plane (Fig. 8).

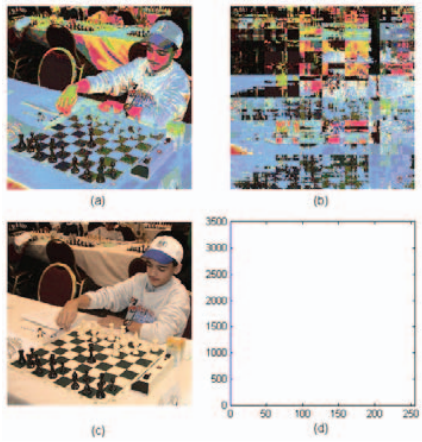

Fig. 7. Color image Encryption with *n=2, p=0* for both GPGC decomposition and encryption. (a) decomposed color image; (b) Encrypted color image; (c) Reconstructed color image; (d) Histogram of the difference between reconstructed color image and original color image.

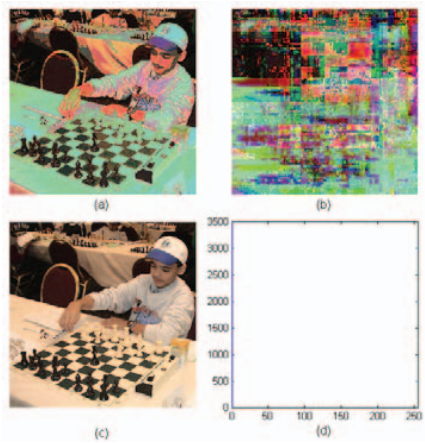

Fig. 8. Color image Encryption with different security keys for each color plane; GPGC decomposition (Red: *n=2, p=0*, Green: *n=2, p=1*, Blue: *n=2, p=2*) and encryption (Red: *n=2, p=1*, Green: *n=3, p=1*, Blue: *n=4, p=1*). (a) decomposed color image; (b) Encrypted color image; (c) Reconstructed color image; (d) Histogram of the difference between reconstructed color image and original color image.

The original color image can be completely reconstructed since there is no difference between the original image and the reconstructed image based on the histogram of the difference between them (shown as Fig. 7(d) and Fig. 8(d)). This demonstrates that our encryption approach is lossless.

V. Security Analysis

The security issues of the presented encryption algorithms are discussed in the section.

A. Security Keys

The base n and parameter p act as security keys for both GPGC decomposition process and encryption process. These security keys are important for users to reconstruct the original images. Fig. 9 shows that the original image can be completely reconstructed only when the correct security keys are being used.

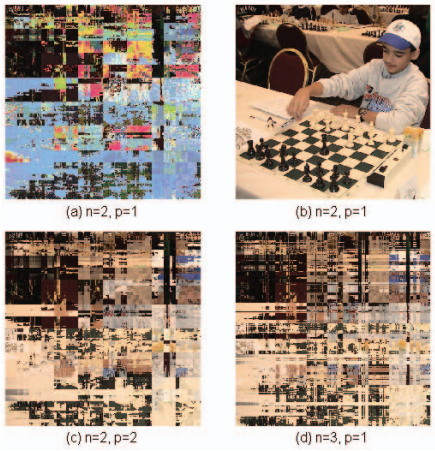

Fig. 9. Color image decryption using different security keys. (a) Encrypted color image with $n=2$, $p=0$ for decomposition and $n=2$, $p=1$ for encryption process; (b) Reconstructed color image using $n=2$, $p=0$ for decomposition and $n=2$, $p=1$ for encryption process; (c) Reconstructed color image using $n=2$, $p=0$ for decomposition and $n=2$, $p=2$ for encryption process; (d) Reconstructed color image using $n=2$, $p=0$ for decomposition and $n=3$, $p=1$ for encryption process.

B. Plaintext Attacks

There are two types of plaintext attacks: the known-plaintext attack and the chosen-plaintext attack. In the cryptography, the plaintext is the original information to be encrypted. The ciphertext is the encrypted plaintext by an encryption algorithm.

The known-plaintext attack is an attack model in which an attacker tires to get the security keys of encryption algorithm by studying a number of plaintexts and their corresponding ciphertexts. On the other hand, the chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then get their corresponding ciphertexts. As a result, the attacker can choose any useful information as the plaintext in order to deduce the security keys of encryption algorithms, or reconstruct the original plaintexts from the unknown ciphertexts [10].

The GPGC decomposition is an important process for the presented encryption algorithms. It changes the image data since it scrambles the bit positions in the binary/arbitrary bit sequence representation of the image pixels. Furthermore, the decomposition results change if the security keys are different as shown in Fig. 7(a) and Fig. 8(a). As a result, the presented algorithms can tolerate not only the known-plaintext attack but also the chosen-plaintext attack for the cryptanalysis purposes.

VI. Conclusion

In this paper, we introduced a new parameter-dependant bit plane decomposition scheme for digital images based on the Generalized P-Gray Code. The Generalized P-Gray Code is a k-digit parametric sequence with arbitrary base, n. The number of bit planes will change with different base n. The bit plane is not binary when the base n is greater than 2. The GPGC representation of image pixel value will be different when the base n and parameter p have different values.

We also introduced two image encryption algorithms based on the GPGC decomposition. One method was presented for grayscale image encryption and the other method is used for color image encryption. Experimental results demonstrate that the presented algorithms are lossless encryption approaches and easy to implement. The original images can be perfectly recovered by only using correct security keys. The images can be protected by full or partial encryption to achieve the different requirements of security levels when different security keys are utilized.

The presented algorithms can be used in real-time applications due to the simplicity of processes and implementation. They can also withstand the plaintext attacks since the GPGC decomposition process changes the image data by transforming the image data into their GPGC representation.

References

[1] **Y. H. Zhang, B. S. Kang, and X. F. Zhang, "Image Encryption Algorithm Based on Chaotic Sequence," in *16th International Conference on Artificial Reality and Telexistence--Workshops*, Hangzhou, China, 2006, pp. 221-223.**

[2] **C. Li, and L. Hong, "A New Image Encryption Scheme based on Hyperchaotic Sequences," in *2007 IEEE International Workshop on Anti-counterfeiting, Security, Identification* Xiamen, China, 2007.**

[3] **J. Zou, R. K. Ward, and D. Qi, "A new digital image scrambling method based on Fibonacci numbers," in *2004 IEEE International Symposium on Circuits and Systems*, 2004, pp. III-965.**

[4] **W. Ding, W. Yan, and D. Qi, "Digital Image Scrambling," *Progress in Natural Science,* vol. 11, p. 7, 2000.**

[5] **Y. Zhou, K. Panetta, and S. Aagaian, "Partial Multimedia Encryption with Different Security Levels," in *2008 IEEE Conference on Technologies for Homeland Security*, Waltham, MA, 2008.**

[6] **S. Li, C. Li, G. Chen, N. G. Bourbakis and K.T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication* vol. 23, pp. 212-223, 2008.**

[7] **R. M. Scopigno, and S. Belfiore, "Image Decomposition for Selective Encryption and Flexible Network Services," in *2004 IEEE Global Telecommunications Conference*, Dallas, TX, 2004, pp. 2302-2307.**

[8] **S.S. Yu, and N.P.Galatsanos, "Binary decompositions for high-order entropy coding of grayscale images," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 6, pp. 21-31, 1996.**

[9] **R. Lukac, and K.N. Plataniotis "A Secret Sharing Scheme for Image Encryption," in *2004 International Symposium on Electronics in Marine*, Zadar, Croatia, 2004, pp. 549-554.**

[10] **A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone *Handbook of Applied Cryptography*. New York: CRC Press, Inc., 1997.**