Partial Multimedia Encryption with Different Security Levels

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

Abstract—**This paper presents three multimedia encryption algorithms base on a new Generalized P-Gray Code (GPGC) to protect the surveillance data in homeland security applications. The GPGC is a k-digital parametric sequence suitable for any base, n. It is also called the (n, k, p)-Gray Code where p is a parameter that allows the users to change the distance to yield different Gray Code sequences. The base n and parameter p as security keys have many options to make the encrypted multimedia difficult to decode. This allows the encrypted objects to be protected with high levels of security. The experimental results verify that the presented algorithms are lossless approaches and good at partial multimedia encryption. A method of measuring the percentage of image encryption is introduced and the measure results are also provided to quantify the encryption performance. Experiments demonstrate that the algorithms show good performance for the common attacks. Due to the low complexity of the algorithms, they are also suitable for real-time applications. The principles behind the presented solutions may be applied to various image, audio, and video systems.**

Index Terms—**Generalized P-Gray Code, (n, k, p)-Gray Code, partial multimedia encryption**

I. Introduction

VISUAL surveillance systems and networks make remote video monitoring available for homeland security purposes and also make it easy to transmit and share videos and image data. With the ubiquitous deployment of visual surveillance systems in many important areas such as airports, commercial centers, banks, schools and also militarily strategic places, large amounts of videos and images with security information are generated, transmitted and stored. Providing security for this information becomes an important and urgent issue. Security of image and video data is also very important in many other areas for homeland security, such as secret communications, confidential remote video conference and security information data protection and sharing as well.

In the digital domain, security needs to address three fundamental problems: (1) secure communication, (2) protection of multimedia data, and (3) privacy of multimedia data (for example, in video surveillance). Using encryption methods on the multimedia data makes the information unrecognized and difficult to decrypt for an unauthorized user.

Newton et al. address the privacy threat brought by a facial recognition technique which stores many different facial characteristics and can automatically identify people in video surveillance systems [1]. Several cryptographic techniques to encrypt the facial images are introduced to protect the privacy of people under surveillance. Only authorized personnel with encryption keys can fully access the protected facial images [1-3].

Encryption schemes based on cryptography principles are designed to ensure the confidentiality of images or videos. However, such solutions may not be suitable for securing real-time applications. For example when transmitting large still images or video via public wireless and mobile networks, the encryption/decryption processes require heavy computation and a large amount of computer resources. This is due to the complexity of the encryption algorithms and the nature of the image/video data (size, memory, and complexity).

Efficiently protecting privacy and encrypting still color images or videos in real time applications are usually based on the principle of partial or selective encryption (encrypting only a portion of the data). Partial encryption enables information to be encrypted with different levels of security for different users according to their needs. Recently, several specialized encryption methods have been developed to encrypt images and videos [3-11].

One of encryption methods is based on Gray Code concepts [9-11]. The Gray Code is a reflected binary sequence where two successive code words differ by only one bit position. This Binary Reflected Gray Code (BRGC) is widely used for error correction in digital communication systems. The (n, k)-Gray Code is introduced when the concept of Gray Code is extended by changing base other than binary [12, 13]. It is known as non-Boolean Gray Code where two adjacent elements differ by only one digit and the difference is either +1 or -1 [12]. Ternary Gray Code is one example for this.

Image scrambling is one of the applications that utilize the Gray Code. Ding et al. presented an image scrambling technology based on Gray Code transform [9, 10]. This approach doesn't have security keys. Zou et al. extended their concept and introduced an image scrambling method using Generalized Gray Code transform [11]. This algorithm provides a little more security than the simple gray code in [9, 10]. However, it does not provide a high level of security.

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: Yicong.Zhou@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).

978-1-4244-1978-4/08/$25.00 ©2008 IEEE

In this paper, we further extend the concept of (n, k)-Gray Code in [12] and P-Gray Code in [14] and introduce a new Generalized P-Gray Code (GPGC), also called (n, k, p)-Gray Code. The new multimedia encryption algorithms using the GPGC transforms are also presented in the section 3. The base n and parameter p as security keys have many choices so that the encrypted multimedia data are difficult to be decoded. This allows encrypted objects to be protected with a high level of security.

The presented algorithms can be used for partial encryption of multimedia such as electronic signatures, fingerprints, binary images, grayscale images, medical images and 3-component color images. Experimental results are provided in the section 4.

II. Generalized P-Gray Code and its Transforms

A generalized Gray Code called (n, k)-Gray Code is a k-digital sequence with base n [12]. A P-Gray Code is introduced in our recently work[14]. A matrix approach to calculate the Generalized Gray Code is presented in [9-11].

In this section, we introduce a new p-parameter based Generalized Gray Code called Generalized P-Gray Code (GPGC). To apply this new GPGC to multimedia encryption, several GPGC based transforms are also presented which can be applied to the multimedia data in different ways.

A. Generalized P-Gray Code

Definition 2.1: If $(a_k a_{k-1} \cdots a_2 a_1)_n$ is the k-digital n-base representation of the non-negative integer A, assume a k-digital n-base sequence $G = (g_k g_{k-1} \cdots g_2 g_1)_n$ is satisfied with

$$g_i = \begin{cases} a_k & i = k \\ (a_i + a_{i+p+1}) \bmod n & 0 \le i \le k-p-1 \\ a_i & i > k-p-1 \end{cases} \quad (1)$$

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.

From the definition above, The GPGC will be different based on the n and p values. For example,

1) When n=2, the GPGC is the binary P-Gray Code, also called (2, k, p)-Gray Code.

$$g_i = \begin{cases} a_k & i = k \\ (a_i + a_{i+p+1}) \bmod 2 & 0 \le i \le k-p-1 \\ a_i & i > k-p-1 \end{cases} \quad (2)$$

2) When n=3, the GPGC is the ternary P-Gray Code, also called (3, k, p)-Gray Code.

$$g_i = \begin{cases} a_k & i = k \\ (a_i + a_{i+p+1}) \bmod 3 & 0 \le i \le k-p-1 \\ a_i & i > k-p-1 \end{cases} \quad (3)$$

When p=0, the GPGC of equation (1) reverts to the classical gray code of base n. For example, the GPGC is the classical Gray Code when p=0 and n=2.

$$g_i = \begin{cases} a_k & i = k \\ (a_i + a_{i+1}) \bmod 2 & 1 \le i < k \end{cases} \quad (4)$$

Multimedia encryption (i.e. image encryption) can be done by randomly changing physical positions of the multimedia data. The GPGC can be used for multimedia encryption since it can transfer an integer sequence into its GPGC representation, a permutation sequence.

B. 1-D Generalized P-Gray Code Transform

Definition 2.2: For a non-negative integer sequence $A = \{A_1, A_2, A_3, ..., A_m\}$, the following transformation is called 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.

$$G = (C_p * A) \bmod n \quad (5)$$

where

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

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

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

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, $1 \le i, j \le k$, $0 \le p \le k$.

From the transformation above, the input sequence $\{A_1, A_2, ..., A_m\}$ can be transferred to a different permutation sequence $\{G_1, G_2, G_3, ..., G_m\}$ when the base n and parameter p have different value. For the certain value of n and p, the P-Gray Code sequence of $\{1, 2, 3, ..., m\}$ can be defined by

$$G_p = \{G_{p1}, G_{p2}, G_{p3}, ..., G_{pm}\} \quad (6)$$

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

Definition 2.3: 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 Inverse 1-D GPGC Transform.

$$A = (C_p^{-1} * G) \bmod n \quad (7)$$

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

1-D GPGC transfer can transfer the integer sequence to its

GPGC representation sequence. This transfer can be used to encrypt one dimensional media such as a string, password, audio or speech signals. It can also be used to encrypt 2-D multimedia line by line, for example grayscale images.

C. 2-D P-Gray Code Transform

To encrypt two dimensional objects, such as electronic signatures, fingerprint, medical images, binary images and grayscale images, the 1-D GPGC transform would be too time-consuming because images should be encrypted line by line. The 2-D GPGC transform is a more efficient process than the 1-D GPGC transform because it can encrypt 2-D images by applying the transform only one time. Furthermore, to reconstruct the original image, we simply apply the 2-D inverse transform one time.

Definition 2.4: Let D be the original 2-D multimedia data matrix, T_r be the row coefficient matrix, T_c be the column coefficient matrix. Then the 2-D GPGC Transform is defined as[14]:

$$E = T_r D T_c \tag{8}$$

where E is the encrypted 2-D multimedia data matrix,

The coefficient matrices of the 2-D GPGC Transform can be generated based on the security keys: base n and parameter p. For an $m \times n$ multimedia data, the row coefficient matrix $T_r(m,m)$ can be generated from equation (6)

$$T_r(i,j) = \begin{cases} 1 & (i, G_{pi}) \\ 0 & otherwise \end{cases} \tag{9}$$

where $1 \le i, j \le m$

And the column coefficient matrix $T_c(n,n)$ can be also calculated in the same way.

$$T_c(i,j) = \begin{cases} 1 & (G_{pj}, j) \\ 0 & otherwise \end{cases} \tag{10}$$

where $1 \le i, j \le n$

As an example, the table 2.1 lists some row and column coefficient matrices of an 8x10 image according to different n and p values.

Definition 2.5: Let E be the encrypted 2-D multimedia data matrix, T_r be the row coefficient matrix, T_c be the column coefficient matrix, the following transformation is called Inverse 2-D GPGC Transform.

$$R = T_r^{-1} E T_c^{-1} \tag{11}$$

where R is the reconstructed image matrix.

Definition 2.6: Let $D = (D_i \quad i)$ be a 3-D multimedia data matrix, where D_i is the 2-D data matrix of the i[th] multimedia component. $T_r = (T_{ri} \quad i)$, where T_{ri} is the row coefficient matrix for the i[th] multimedia component defined by function (9). $T_c = (T_{ci} \quad i)$, where T_{ci} is the column coefficient matrix of the i[th] multimedia component defined by function (10). The following transformation is called the 3-D GPGC Transform.

$$E = T_r D T_c \tag{12}$$

where E is the matrix of the Encrypted 3-D multimedia data, and $i = 1, 2, 3$.

TABLE 2.1 THE ROW AND COLUMN COEFFICIENT MATRICES FOR AN 8X12 IMAGE

(n,p)	Row coefficient matrix	Column coefficient matrix
(3,0)	$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}$	$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&1 \end{pmatrix}$
(2,1)	$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \end{pmatrix}$	$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1&0&0 \end{pmatrix}$

Definition 2.7: Let $E = (E_i \quad i)$ be an encrypted 3-D multimedia data matrix, where E_i is the scrambled 2-D data matrix of the i[th] multimedia component. $T_r^{-1} = (T_r^{-1} \quad i)$, where T_{ri}^{-1} is the inverse row coefficient matrix of the i[th] multimedia component. $T_c^{-1} = (T_c^{-1} \quad i)$, where T_{ci}^{-1} is the inverse column coefficient matrix of the i[th] multimedia component. The following transformation is called the Inverse 3-D GPGC Transform.

$$R = T_r^{-1} E T_c^{-1} \tag{13}$$

where R is the reconstructed 3-D multimedia data, and $i = 1, 2, 3$.

III. MULTIMEDIA ENCRYPTION ALGORITHMS

A. 2-D multimedia encryption algorithm

The data of 2-D multimedia consists of 2-D matrices, for example, electronic signatures, binary images, fingerprint, medical images, and grayscale images. Here we provide a multimedia encryption algorithm based on the 2-D GPGC transform which can partially encrypt these types of media data in one step. The encryption algorithm is shown in Fig. 1.

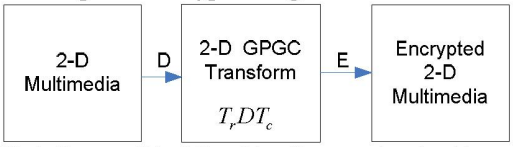

Fig. 1. Block diagram of the 2-D multimedia encryption algorithm

To encrypt the 2-D multimedia data, the security keys: base n and parameter p should be selected first. The row and column coefficient matrices can be calculated according to the

equations (9) and (10). The encrypted 2-D multimedia can be generated by applying the 2-D GPGC transform.

Similarly, to decode the encrypted image, the authorized users should have the security keys: base n and parameter p. They generate the row and column coefficient matrices by using equations (9) and (10), then obtain their inverse matrices. The original image can be recovered by applying inverse 2-D GPGC transform (shown in Fig. 2).

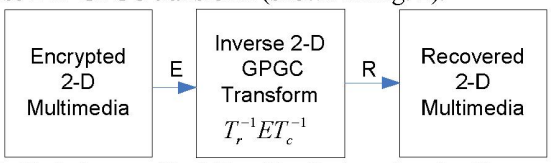

Fig. 2. Block diagram of the 2-D multimedia decryption algorithm

B. 3-D multimedia encryption algorithms

3-D multimedia data has 3 dimensional data matrices. For example, in the color images, the 3-dimension data matrices represent three separate color planes. The data for each color plane is a 2-D data matrix. We introduce two algorithms to encrypt such types of multimedia data.

The first algorithm (shown in figure 3) uses the 2-D GPGC transform. The 3-D multimedia data matrix is separated into three 2-D component data matrices. The 2-D GPGC transform is applied to encrypt each component individually. The encrypted 3-D multimedia data can be generated by combining the three encrypted components.

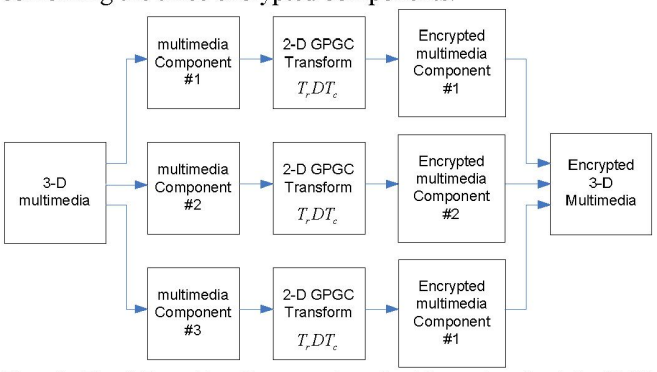

Fig. 3. The 3-D multimedia encryption algorithm using the 2-D GPGC transform

The second algorithm (shown in figure 4) is based on 3-D GPGC transform in definition 2.6. The encrypted 3-D multimedia data can be generated after directly applying 3-D GPGC transform. The user can choose the same security keys n and p for all three multimedia components, or have the flexibility to choose different security keys for each multimedia component.

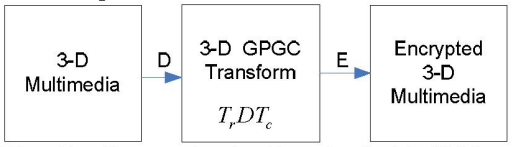

Fig. 4. 3-D multimedia encryption algorithm using the 3-D GPGC transform.

On the other hand, the encrypted multimedia data can be decrypted by using the inverse 2-D or 3-D GPGC transform. By using the inverse 2-D GPGC transform, the encrypted multimedia data matrix should be separated into three 2-D multimedia components. The three multimedia components can be reconstructed by individually applying the inverse 2-D GPGC transform. Combing these three reconstructed components gets the reconstructed 3-D multimedia data.

Similar to the encryption process, decrypting the multimedia data can also be done via the inverse 3-D GPGC transform. The reconstructed multimedia data can be generated by directly applying the inverse 3-D GPGC transform to the encrypted multimedia data.

IV. Experimental Results of Multimedia Encryption

A. 2-D multimedia encryption

2-D multimedia data consists of 2-D matrices such as those found in electronics signatures, fingerprints, medical images, binary images, and grayscale images. To encrypt the 2-D data, the 2-D GPGC transform is applied to the 2-D multimedia data based on definition 2.4. Figure 5 shows an example of the grayscale image encryption with security keys: base n=3, p=0. The experimental results show that the original image can be perfectly reconstructed. This can be verified from the histogram of the difference between the reconstructed image and the original image (Figure 5(f)).

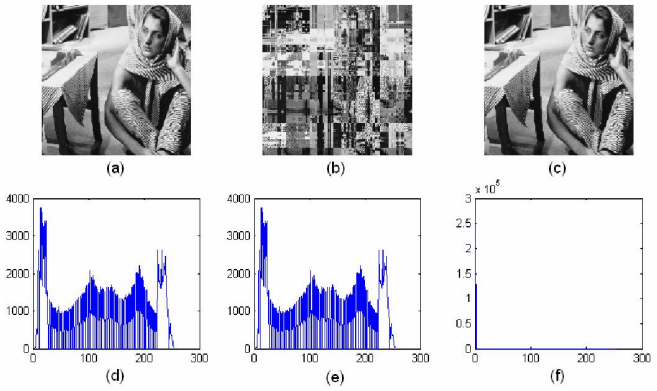

Fig. 5. Gray image encryption with base n=3 and p=0. (a) Original gray image; (b) Encrypted gray image; (c) Reconstructed gray image; (d) Histogram of original gray image; (e)Histogram of encrypted image; (f) Histogram of the difference between reconstructed gray image and original gray image.

More encryption examples of the 2-D multimedia encryption are provided with different base n and p values in figure 6 (fingerprint encryption), figure 7 (medical image encryption), and figure 8 (binary image encryption).

These encrypted results show that as the p value increases, the amount of multimedia encryption decreases. Higher p values result in the multimedia data being more recognizable than the results generated where p has lower value. This is because for smaller value of p, the number of image pixel permutations increases. Similarly, the percentage of multimedia encryption also decreases if base n goes higher. The digital of sequence representation will be shorter when base n increases. The result is the same as that of higher p value.

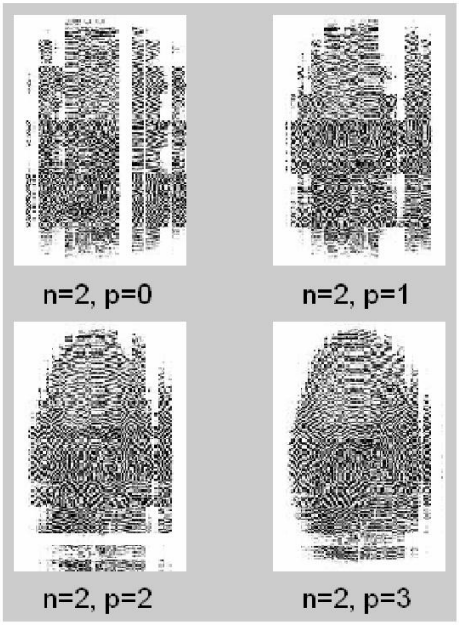

Fig. 6. Encrypted fingerprints with base n=2 and different p values

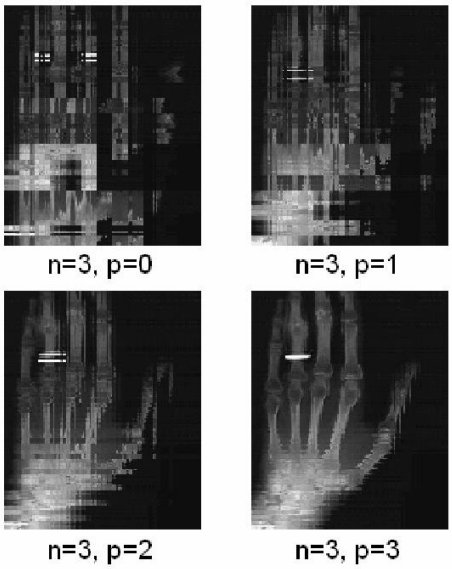

Fig. 7. Encrypted medical images with base n=3 and different p values

Fig. 8. Encrypted binary images with base n=3 and different p values

B. *Color image encryption results*

Fig. 9. Encrypted color images with base n=2 and different p values

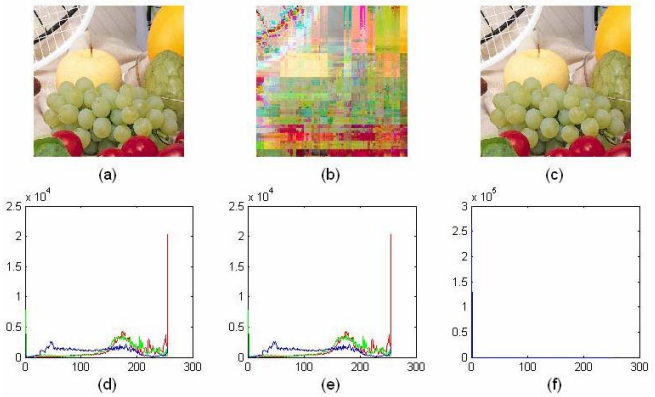

Fig. 10. Encrypted color image with base n=3 and Red: p1=0; Green: p2=1; Blue: p3=2. (a) Original color image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of original color image; (e)Histogram of encrypted image; (f) Histogram of the difference between reconstructed color image and original color image.

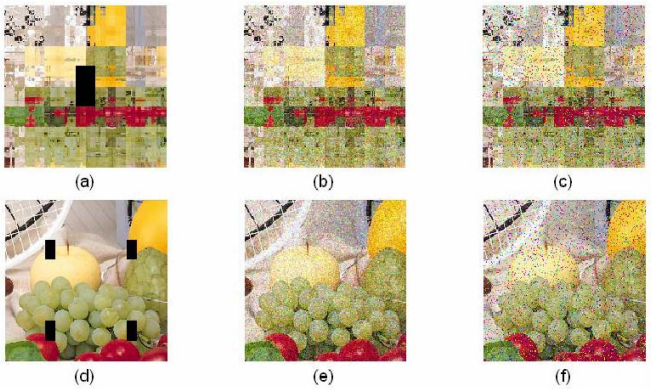

Fig. 11. Encrypted images with n=2, p=0 and reconstructed images after image attacks. (a) Encrypted images with 128x64 cutting attack; (b) Encrypted images with 12.5% Gaussian noise; (c) Encrypted images with 10% Salt&pepper noise; (d) Reconstructed images form (a); (e) Reconstructed images from (b); (f) Reconstructed images from (c).

3-D multimedia data such as color images can be encrypted by using either the 2-D GPGC transform or the 3-D GPGC transform. The users have the flexibility to use the same security keys for all color components (Figure 9) or choosing a different p value for each color component (Figure 10). Figure 9 gives the encrypted examples where base n=2 with

the p value changing. The better encryption results are obtained where p has a smaller value. The original image can be completely (Figure 10) recovered since there is no difference between the original image and the recovered image based on the histogram of the difference between them (Figure 10(f)). This shows that our approach is lossless.

The presented image encryption algorithms have good performance in common image attacks as demonstrated by the experimental results shown in Figure 11. The reconstructed images have some distortion due to the attacks. However, we can see what the original image is since the reconstructed images contain almost all the visual information contained with in original images.

V. The Percentage of Image Encryption and Measure Results

Wang et al. present an approach to measure the structural similarity (SSIM) between the measured image and the reference image [15]. The measure result is 1 if the measured image is the same as the reference image. On the contrary, the result will be zero if the measured image is totally different with the reference image. This method can be extended to measure the percentage of image encryption for the partial encryption or selective encryption of images. The percentage of image encryption can be calculated the difference of the encrypted image and the original image.

Definition 6.1: Let $SSIM(x, y)$ be the structure similarity index defined in [15], the following definition

$$Percentage = (1 - SSIM(x, y)) \times 100\% \qquad (14)$$

is called the percentage of image encryption.

The measure examples are shown in Figure 12. The results show that the better encryption can be achieved with smaller values of n and p.

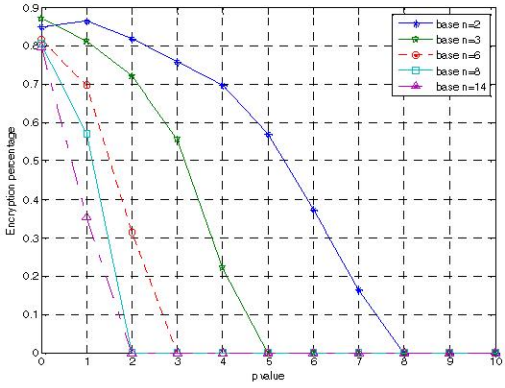

Fig. 12. Percentage of Image Encryption of the Lena image with different p values.

VI. Conclusion

We introduced a new Generalized P-Gray Code called (n, k, p)-Gray Code and also the new multimedia encryption algorithms based on a 2-D GPGC transform and a 3-D GPGC transform in this paper. The security keys, base-n and parameter p, have many possible choices which provide the multimedia data with a high level of security. The presented approaches are lossless and good at partial encryption of images which are demonstrated in experiments. We also introduced a new measure method of the percentage of image encryption. The measure results show that image can be encrypted in wide and flexible ranges based on different security keys. The algorithms can be implemented for 2-D and 3-D multimedia data. They can also be used in real-time applications, such as encrypting pay TV, video and speech. Experimental results showed that the algorithms have good performance in common image attacks.

References

[1] Elaine M. Newton, Latanya Sweeney and Bradley Malin, "Preserving privacy by de-identifying face images," *Transactions on Knowledge and Data Engineering,* vol. 17, pp. 232-243, 2005.

[2] T.E. Boult, "PICO: Privacy through Invertible Cryptographic Obscuration," in *IEEE/NFS Workshop on Computer Vision for Interactive and Intelligent Environment*, 2005.

[3] Frédéric Dufaux and Touradj Ebrahimi, "Scrambling for Video Surveillance with Privacy," in *Conference on Computer Vision and Pattern Recognition Workshop*, New York City, 2006, pp. 160-160.

[4] Darko Kirovski Borko Furht, "Multimedia Security Handbook ": CRC, 2004.

[5] Wenjun Zeng and Shawmin Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE TRANSACTIONS ON MULTIMEDIA,* vol. 5, pp. 118-129, 2003.

[6] Xiliang Liu and Ahmet M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," in *Second IASTED International Conference on on Communications, Internet and Information Technology* Scottsdale, AZ, USA, 2003, pp. 527-533.

[7] Bin B. Zhu, Mitchell D. Swanson and Shipeng Li, "Encryption and authentication for scalable multimedia: Current state of the art and challenges," in *Proceedings SPIE International Symposium Information Technology & Communication* Philadelphia, PA USA, 2004, pp. 157-170.

[8] Zhaoyu Liu, Yuliang Zheng, Edd Hauser, Jeffrey Liu and E. Winters Mabry, "Secure Internetworking Video Surveillance for DHS Protection Mission," in *the Department of Homeland Security Conference-Working Together: Research & Development (R&D) Partnerships in Homeland Security*, Boston, MA, USA, 2005.

[9] W. Ding, W. Q. Yan, D. X. Qi, "Digital Image Scrambling Technology Based on Gray Code," in *Proc. of International Conference on CAD/CG*, 1999.

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

[11] Jiancheng Zou and Rabab K. Ward, "Introducing two new image scrambling methods," in *Proc. IEEE PacRim Conf. Comm. , Comp., and Sig. Proc.*, 2003, pp. 708-711.

[12] Dah-Jyh Guan, "Generalized Gray Code with applications," *Proc. Natl. Sci. Counc. ROC(A),* vol. 22, pp. 841-848, 1998.

[13] K. Jaya Sankar, V. M. Pandharipande and P. S. Moharir, "Generalized Gray Codes," in *ISPACS 2004. Proceedings of 2004 International Symposium on ,*, 2004, pp. 654-659.

[14] Yicong Zhou, Karen Panetta and Sos Agaian, "P-recursive sequence and key-dependent multimedia scrambling," in *Mobile Multimedia/Image Processing for Military and Security Applications, SPIE Defence and Security Symposium 2008* Orlando, FL USA 2008.

[15] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh and Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing,* vol. 13, p. 13, APRIL 2004.