Key Independent Decryption of Graphically Encrypted Images

Ram Ratan

Defence Research and Development Organisation
Scientific Analysis Group, Metcalfe House Complex, Delhi-110054
India
ramratan_sag@hotmail.com

Abstract. Cryptographically, an encryption algorithm should be strong enough so that one could not extract any information from encrypted data. A graphical encryption method proposed in [1] for the security of computer data is cryptanalysed in this paper. There are some regions left unchanged and clearly visible in graphically encrypted images. Key independent decryption of graphically encrypted images is proposed for recovery of intelligible information. Decryption scheme is based on neighbourhood similarity characteristics of adjacent pixels. Simulation results show that the decrypted images obtained by the proposed scheme are quite intelligible to understand. The graphical encryption method in present form is not suitable for security applications as encrypted images can be decrypted easily.

Keywords: Image Secrecy, Graphical Encryption, Image Decryption, Neighbourhood Similarity, Visual Perception.

1 Introduction

Security of information is an important issue in design and development of secure information management systems for reliable communication and storage of sensitive information. Nowadays in the digital world, digital images apart from other form of information are commonly used by modern societies. There are many ways: spread spectrum, steganography and cryptography for achieving security of such information. Encryption is the process which transforms the plain image with the use of encryption key into encrypted form which is unintelligible and looks like random mesh of pixels. Image encryption has wide applications in various areas like strategic communication, telemedicine, medical imaging and multimedia systems for secure management of visual information. The images are different from the normal text and it is not a wise idea to use traditional encryption schemes to encrypt them because of much encryption time of large image size. Moreover, decrypted text must be same as plain text but this is not necessary for images because of visual characteristics of human perception which tolerate small errors in decrypted images.

H. Chen et al. (Eds.): PAISI 2010, LNCS 6122, pp. 88–97, 2010.

Various encryption schemes have been reported in the literature for achieving the security of images which can be classified in three types as position permutation, value transformation and visual transformation [1-5]. Present paper is concerned with value transformation based encryption in which the pixel values are transformed by drawing the lines randomly in inversion mode on image plane, i.e., black pixel becomes white or vice versa. This method of encryption is known as graphical encryption method for encryption of computer data [1].

Cryptanalysis of such encryption methods for recovery of plain information from encrypted images is very important in various applications like interception analysis for extraction of meaningful information and also in assessing security of encryption schemes. Decryption is the process by which plain information is recovered from given encrypted information with the use of decryption key. Decryption is very difficult in the absence of decryption key to recover plain information. Cryptanalytically, decryption should be simple and fast so that one can recover meaningful and intelligible information from given encrypted data with minimum efforts. Exploitation of weaknesses observed in encryption method, reduction of number of trails in exhaustive method of decryption and recovery of any plain information even in partial or in distorted form are also the appreciable achievements. Depending on the situations, following attacks can be considered in the cryptanalysis of encryption methods: (1) Known cipher image (2) Chosen cipher image (3) Known plain image and (4) Chosen plain image. Cryptographically, the attacks should not be applicable in any case on the encryption method developed for security applications.

A graphical method of encryption was cryptanalysed in [6] for obtaining original data from given ciphertext under known and chosen plaintext conditions. The mask key data is obtained from a pair of plaintext (chosen/known) and ciphertext by $'XOR'$ operation and this mask key data is $'XOR'$ with given ciphertext to obtain original data. This attack is applicable only when ciphertext of chosen/known plaintext and given ciphertext which is to be decrypted are obtained with same encryption key. Graphical encryption method in which horizontal/vertical lines along with few random lines were drawn was also analysed for recovery of text documents by computing line to line correlation and applying Fuzzy character recognition under known cipher image situation [7].

In this paper, we present some observations: presence of unchanged regions in encrypted images, inversion of pixels several times etc. and propose the key independent decryption scheme for recovery of graphically encrypted gray level images when only an encrypted image is known. The point, local and global operations like image smoothing, edge enhancement etc. for enhancement of images and also for extraction of features like edge extraction, region segmentation etc. for analysis of images which are useful in many image processing applications are available in the literature [8-10]. These operations are not applicable directly in decryption of encrypted images because of random messing and high distortion in such images. For decryption of such graphically encrypted images, we require to invert the pixels again along random lines as drawn during encryption. For this, we need seed of random number generator used during encryption to get same line points for drawing same lines and inverting pixels along drawn lines. In this paper, we decrypt such encrypted images without any knowledge of decryption key. Two cases, first one random lines drawing and another horizontal/vertical lines drawing used during encryption are considered for decryption. Decryption scheme proposed is based on neighbourhood similarity characteristics of adjacent pixels where point-to-point operation for random lines and line-to-line operation for horizontal/vertical lines are performed. Decryption scheme proposed for decryption of images encrypted with random lines drawing is also applicable for any kind of pixel inversion based encryption to decrypt such encrypted images.

The paper is organized as follows: First we give a brief introduction of graphical encryption method in Section 2. The cryptographic observations on graphical image encryption are presented in Section 3. Decryption scheme proposed for recovery of intelligible information from given graphically encrypted image is presented in Section 4. The simulation results obtained for some encrypted images are presented in Section 5. Finally, the paper is concluded in Section 6 followed by the references.

2 Graphical Encryption

Computer data which is to be encrypted is displayed on computer monitor. Graphical encryption method uses two computer functions: (1) random number generation, and (2) drawing of line in inversion mode with a pen of size $1 \times 1, 2 \times 2$ etc. between two points on the image plane. As per inversion, the black pixel becomes white and vice versa during graphical encryption. The seed of random number generator is known as the key which is needed during encryption and decryption. Random number generator generates a sequence of random numbers as coordinates of end points of lines which are to be drawn on image plane. As the number of lines increases during encryption, the intelligibility of encrypted image reduces. The process of drawing line in inversion mode is repeated until the intelligibility of image vahishes. Detailed description of this method can be found in [1]. This method is applied for encryption of gray level images where the darker pixels become brighter and vice versa [11]. Decryption of encrypted images is performed with the same key, pen size and number of lines as used in encryption to obtain the original images. As an example, encrypted images obtained for some plain images are shown in *figure 1.*

3 Observations on Graphical Encryption

Graphical encryption method has several good characteristics for encryption: (1) easy to implement, (2) easy assignment of encryption key, (3) non propagation of error, and (4) non expansion of encrypted data. Although graphical encryption method has above advantages but following observations show some disadvantages: (1) pixels are inverted many times depending on number of lines passing through these pixels, (2) unintelligibility of encrypted image depends on number of lines drawn, (3) Nearly half of the pixels in encrypted image remain

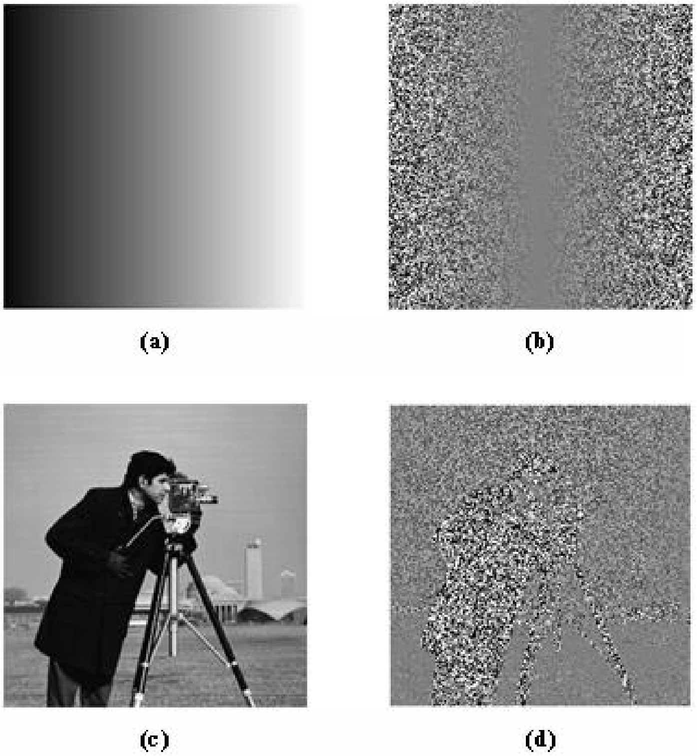

Fig. 1. Graphically encrypted images showing presence of unchanged regions : (a),(c) plain images; and (b),(d) encrypted images

unchanged, (4) Regions having pixel values near to middle of range in plain image remain visually unchanged and visible in encrypted image.

Let f be an image of size $M \times N$, $f(x, y), 1 \leq x \leq M, 1 \leq y \leq N$, be the pixel value at (x, y) position. $f(x, y)$ lies between 0 to L where L is the range of pixel values and this is 255 for 8 bit gray level image. Let encrypted image is f' which is obtained by applying graphical encryption on f. The regions of plain image which have $f(x, y)$ near to $L/2$ remain unchanged in f'. The *figure 1* shows unchanged regions in f. An image of *figure 1(a)* is the simulated picture where pixel values vary from 0 to 255 starting from left to right. And an image of *figure 1(c)* is the actual picture. In *figure 1*, it is seen that the vertically middle portion of *figure 1(a)* appears unchanged as shown in *figure 1(b)* and some patches of *figure 1(c)* appear unchanged as shown in *figure 1(d)*.

Similar results as of graphical encryption method can be obtained easily by generating a random binary matrix b of same size as of f through random number generator and inverting randomly selected pixel $f(x, y), 1 \leq x \leq M, 1 \leq y \leq N$, once only depending on $b(x, y)$ of b. $f(x, y)$ is to be inverted if $b(x, y) = 1(0)$ otherwise remains unchanged, i.e., if $b(x, y) = 1(0)$ then $f'(x, y) = L - f(x, y)$

else $f'(x,y) = f(x,y)$. In this manner, the pixels of f chosen randomly are to be inverted once only to get f'.

4 Image Decryption Scheme

We see in images that the value of pixels is normally varying smoothly in neighbourhood regions. This property of plain images can help us in decryption to recover intelligible information from given encrypted images. Divide and conquer attack can make the solution efficient to given complex problem by decomposing it into simple problems. Normally, we require decryption key (seed, pen size and number of lines as used in encryption) to decrypt such encrypted images, but decryption scheme proposed is independent of key. We take two cases, one is random lines drawing and another is horizontal/vertical lines drawing where key information is not available for decryption of graphically encrypted images.

As per divide and conquer attack, we process pixel-by-pixel and line-by-line for random lines drawing and horizontal/vertical lines drawing respectively. The neighbourhood similarity applied here is the difference between two adjacent pixels (lines) which is used to correct pixels (lines) by inverting function to decrypt encrypted image. Let f' is the given encrypted image and g is the decrypted image. The decryption process for recovery of information from graphically encrypted image with random and horizontal/vertical lines drawing is described as follows:

4.1 Decryption of Image Encrypted with Random Lines Drawing

```
//Processing of pixels starting from second pixel
 of column one//
  for x = 2 to M
  begin
     diff1 = |f'(x,1) - f'(x-1,1)|
     diff2 = |(L-f'(x,1)) - f'(x-1,1)|
     if (diff1 > diff2) then g(x,1) = L - f'(x,1)
     else g(x,y) = f'(x,y)
  end
//Processing of pixels starting from first row and
second column//
  for x = 1 to M
  for y = 2 to N
  begin
     diff1 = |f'(x,y)-f'(x,y-1)|
     diff2 = |(L-f'(x,y))-f'(x,y-1)|
     if (diff1 > diff2) then g(x,y) = L-f'(x,y)
     else g(x,y) = f'(x,y)
  end
```

4.2 Decryption of Image Encrypted with Horizontal/Vertical Lines Drawing

```
//Processing of rows starting from second row//
  for x = 2 to M
  begin
     diff1 = |row(x) - row(x-1)|
     //(pixel by pixel sum of absolute difference of
      pixel values)//
     diff2 = |L-row(x) - row(x-1)|
     if (diff1 > diff2) then row(x) = L-row(x)
  end
//Processing of columns starting from second column//
  for y = 2 to N
  begin
     diff1 = |column(y) - column(y-1)|
     diff2 = |L-row(y) - row(y-1)|
     if (diff1 > diff2) then column(y) = L-column(y)
  end
```

We start processing of encrypted image from second pixel $f'(1,2)$ based on previous pixel $f'(1,1)$ in case of random lines drawing and from second row based on previous row in case of horizontal/vertical lines drawing. It is not known here whether the first pixel (first row) is inverted or not during encryption. We get decrypted image g as a negative of plain image f if first pixel (first row) was inverted and we get g as a plain image if first pixel (first row) was not inverted during encryption. So we obtain two decrypted images, both have intelligible information, in which one of them has good visual perception similar to plain image. Decryption process discussed for random lines drawing can also be considered for decryption of images encrypted with any kind of drawing and pixel inversion.

5 Simulation Results and Discussions

Proposed decryption scheme for graphically encrypted images is implemented in MATLAB programming on MATLAB Platform. Scheme provides intelligible decrypted images with good visual perception. The decrypted images are same to the originals in case of encryption with horizontal/vertical lines drawing and quite intelligible also in case of encryption with random lines drawing. Proposed decryption scheme is tested for decryption of various encrypted images. As an example, decrypted images obtained for some images encrypted with horizontal/vertical lines drawing and random lines drawing are shown in *figure 2* and *figure 3* respectively. Decrypted results shown in *figure 3* are obtained for plain images (a)-(d) of *figure 2*

The error in decrypted image is measured as mean square error (MSE) which is computed as

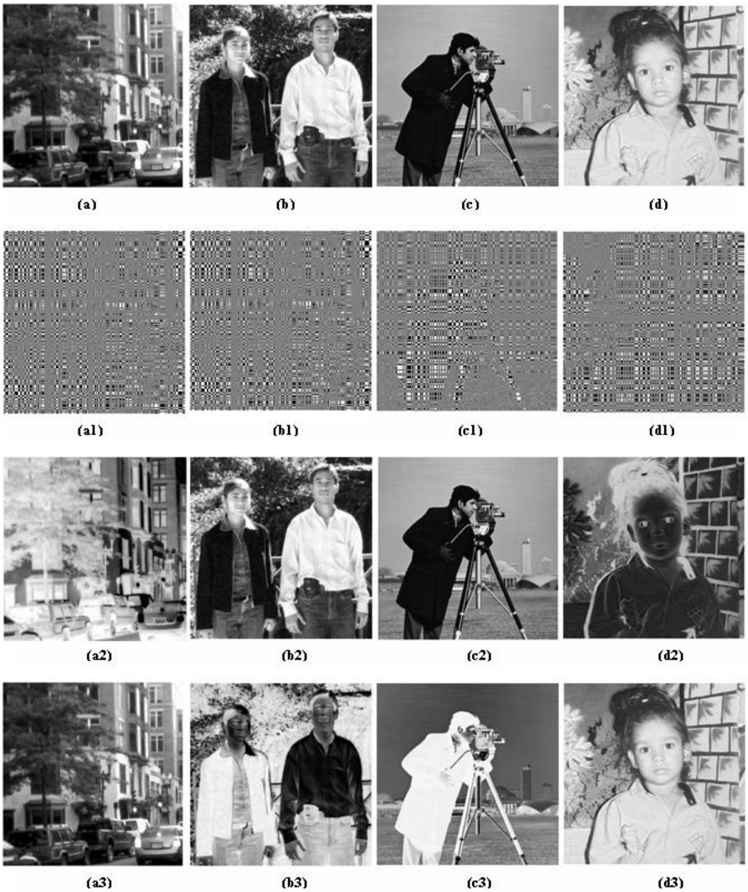

Fig. 2. Decryption of images graphically encrypted with horizontal/vertical lines: (a)-(d) plain images; (a1)-(d1) encrypted images of (a)-(d); (a2)-(d2) decrypted images; and (a3)-(d3) images as negative of (a2)-(d2)

$$MSE = \frac{1}{M \times N}[f(i,j) - g(i,j)]^2, 1 \leq i \leq M \text{ and } 1 \leq j \leq N.$$

Error measured as MSE in decrypted images does not reduce considerably from the error in encrypted images in case of random lines drawing encryption but it reduces to zero in case of horizontal/vertical lines drawing encryption. MSE measured in different encrypted and decrypted images is shown in *Table 1*. From *figure 2* and *Table 1*, it is clear that in case of horizontal/vertical lines drawing encryption the decrypted images which look same as to original have zero MSE and others have larger MSE even compared to MSE in encrypted images. From *figure 3* and *Table 1*, it is also clear that in case of random lines drawing encryption the decrypted images which have larger MSE even compared to MSE in encrypted images look fine whereas others have lesser MSE. Decryption scheme

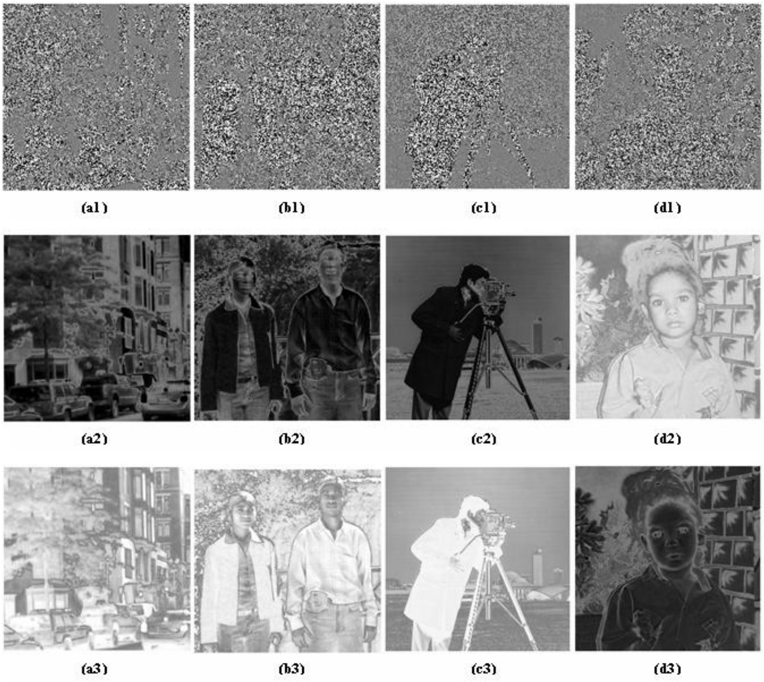

Fig. 3. Decryption of images graphically encrypted with random lines: (a1)-(d1) encrypted images of figure 2(a)-(d); (a2)-(d2) decrypted images; (a3)-(d3) images as negative of (a2)-(d2)

proposed for decryption of random lines drawing based encrypted images is also applied for decryption of horizontal/vertical lines drawing based encrypted images. The results are shown in *figure 4* where visual quality of such decrypted images is also quite intelligible. These results show that the decryption scheme proposed for decryption of encrypted images with random lines drawing is applicable also for any kind of pixel inversion based encryption to decrypt such encrypted images.

Security of graphical encryption method depends on the seed of random number generator which is used to obtain end points of lines for inverting pixels along lines drawn during encryption and decryption. In absence of key and fixed lines/pensize, we have to apply 2^{32} number of trials in exhaustive method for 32 bit seed to get the plain image. As the decryption scheme proposed is independent of key and does not require key information, the scheme decrypts encrypted image in one pass only for random lines drawing encryption case and in two passes only for horizontal/vertical lines drawing encryption case. Simulated results show that the graphical encryption method is insecure in present form. The graphical encryption can be made secure against above attacks by incorporating pixel masking, pixel substitution and pixel permutation [12-15].

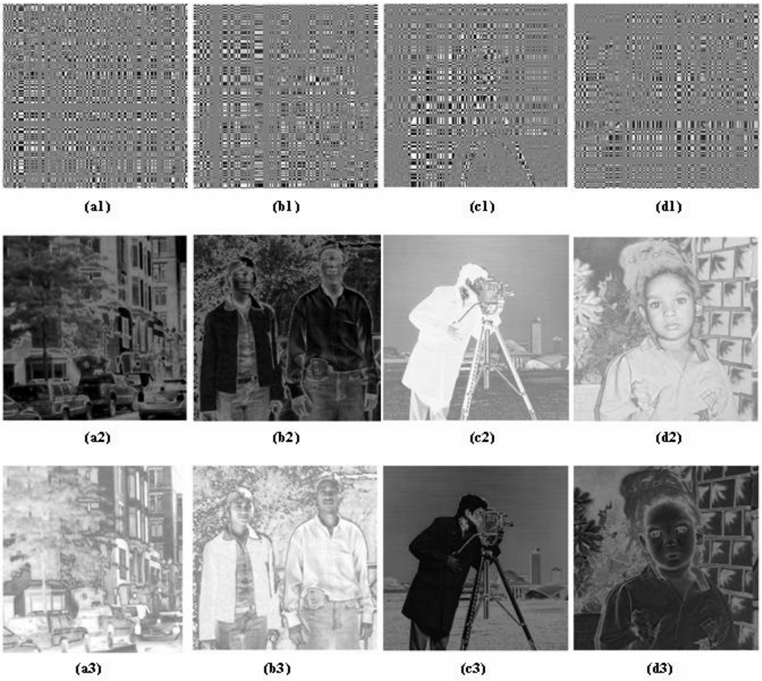

Fig. 4. Decryption of images encrypted with horizontal/vertical lines by scheme proposed for decryption of images encrypted with random lines: (a1)-(d1) images of figure 2(a)-(d) encrypted with horizontal/vertical lines; (a2)-(d2) decrypted images; and (a3)-(d3) images as negative of (a2)-(d2)

Table 1. MSE measured in different images

Plain images for simulation	MSE in case of horizontal/vertical lines drawing			MSE in case of random lines drawing		
	Encrypted images	First decrypted image	Second decrypted image	Encrypted image	First decrypted image	Second decrypted image
Street	9651	19260	0	9613	14849	4411
Children	13897	0	27866	13984	17007	10853
Cameraman	8687	0	17284	8611	13215	4069
baby	8972	17956	0	9014	1981	15975

6 Conclusion

The decryption scheme presented in this paper for decryption of graphically encrypted images is automatic and independent of key. The scheme of decryption is based on divide and conquer attack in which neighbourhood similarity between adjacent pixels or lines has been used. It has been shown in simulation results that encrypted images can be decrypted easily without the knowledge of decryption key with good intelligibility. The images encrypted with horizontal/vertical lines drawing can be decrypted as original and the images encrypted with random lines drawing can also be decrypted with good visual perception. Further, it has been shown that decryption scheme proposed for decryption of images encrypted with random lines drawing is applicable for any kind of pixel inversion based encryption to decrypt such encrypted images with good perception. Hence, graphical encryption method in present form is insecure and should not be used for security applications.

References

1. Schwartz, C.: A new graphical method for encryption of computer data. Journal of Cryptologia 15(1), 43–46 (1991)
2. Bourbakis, N.G., Alexopoulos, C.: Picture data encryption using scan patterns. Pattern Recognition 25(6), 567–581 (1882)
3. Maitra, A., Rao, Y. V. S., and Prasanna, S. R. M.: A new image encryption approach using combinational permutation techniques. International Journal of Computer Science, 19(2), 127-131, (2006)
4. Maniccam, S.S., Bourbakis, N.G.: Image and video encryption using scan patterns. Pattern Recognition 37(4), 725–737 (2004)
5. Yen, J.-C., Guo, J.-I.: A new image encryption algorithm and its VLSI architecture. In: Proceedings of IEEE Workshop Signal Processing Systems, pp. 430–437 (1999)
6. Chin, Y.-C., Wang, P.-C., Hwang, J.-J.: Cryptanalysis on Schwartz graphical encryption method. Journal of Cryptologia 17(3), 301–304 (1993)
7. Ratan, R., Saxena, P.K.: An algorithm for the restoration of distorted text documents. In: Proceedings of Intl. Conference on Computational Linguistics, Speech and Document Processing (ICCLSDP'98), pp. A38–A43 (1998)
8. Jain, A.K.: Fundamentals of digital image processing. Prentice Hall, Englewood Cliffs (1995)
9. Russ, J.C.: The image processing handbook. CRC Press, Boca Raton (1995)
10. Young, T.Y., Fu, K.S.: Handbook of pattern recognition and image processing. Academic Press, London (1986)
11. Ratan, R., Saxena, P.K.: Image processing based techniques for securing text documents. Journal of Discrete Mathematical Sciences and Cryptography 3(1-3), 113–129 (2000)
12. Fu, C., Zhu, Z.: A chaotic encryption scheme based on circular bit shift method. In: Proceedings of Intl. Conference for Young Computer Scientists, pp. 3057–3061. IEEE Computer Society, Los Alamitos (2008)
13. Menezes, A.P., Van Oorschot, Vanstone, S.: Handbook of applied cryptography. CRC Press, Boca Raton (1996)
14. Schneier, B.: Applied cryptography. John Wiley & Sons Inc., Chichester (1996)
15. Yen, J.C., Guo, J.I.: A new chaotic key based design for image encryption and decryption. In: Proceedings of IEEE International Symposium Circuits and Systems, vol. 4, pp. 49–52 (2000)