Advances in Intelligent Systems Research, volume 174

Proceedings of the 8th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2020)

Data Protection of Multimedia Content for E-Learning Using Discrete Wavelet Transform

Andrey Zemtsov*
Department of Computers and Systems
Volgograd State Technical University
Volgograd, Russian Federation
ecmsys@yandex.ru

***Abstract*—The issues of assessment of images watermarking using discrete wavelet transform in the e-learning system is considered in the article. A digital watermark is primarily hidden data that is embedded inside a digital image, video, audio, or any other digital container. If the container with the embedded watermark was stolen, then the watermark will be present in it, which will help to track the fact of illegal distribution of the protected digital document or confirm the rights of the original owner. An attacker may try to remove a watermark to illegally assign a digital document. Therefore, one of the tasks when implementing a watermark is to ensure its resistance to removal. Embedding is performed in the low-frequency domain of the wavelet spectrum. The experimental results are showing the possibility of using the considered image watermarking method for solving data protection of multimedia content problems are presented. The application of the implemented method under consideration for use in conjunction with modern compression formats is justified.**

Keywords—copyright protection; watermarking; e-learning; wavelet transform; quality metrics, PSNR

I. INTRODUCTION

The All-Russian survey of teachers conducted by the NAFI Analytical Center (nafi.ru) from March 20 to 27, 2020, during which 1,100 Russian teachers were surveyed, showed that despite all the efforts made, during the transition to distance learning due to the coronavirus pandemic it became obvious that many educational organizations are not even ready for a partial transition to e-learning using distance learning technologies. Nevertheless, today the need for the use of Internet resources and technologies in education is not in doubt.

Existing e-learning systems were not ready to provide teachers with the necessary functionality, and also could not withstand the communication load, because were not designed for the mass connection of students of distance learning courses. The vast majority of such e-learning systems are based on the Learning Management System platform such as ATutor, Claroline, Dokeos, LAMS, Moodle, OLAT, OpenACS, Sakai, and others. In many educational institutions, e-learning systems were absent at the onset of the coronavirus epidemic. As a result, for distance learning, teachers massively used third-party solutions such as Zoom, Skype, YouTube, and webinar rooms, including instead of existing e-learning systems.

The transition to e-learning using distance learning technologies in the context of the coronavirus pandemic will lead to a change in the education system at all levels throughout the world. Practical experience has convincingly demonstrated that the use of Internet technologies in the organization of training leads to a significant increase in accessibility and quality and, as a result, helps to increase the profitability of training systems. The e-learning system should provide each student with information and educational opportunities at any time at the point of presence. In other words, the Internet-oriented model of education is characterized by complete freedom from space-time restrictions and accessibility for all interested students, regardless of their location. With the development of communication solutions, in conditions of the impossibility of providing absolute control of communication channels, the protection of transmitted multimedia content becomes especially relevant.

II. THREATS AND RISKS IN THE E-LEARNING SYSTEM

Courses designed for e-learning contain new types of distributed educational materials using the advantages of a network, multimedia, and other information technologies. At the same time, the issue of copyright protection, intellectual property, authentication, and student identification in the provision of distributed educational materials through open communication channels remains relevant. The advantages of providing and transmitting knowledge in digital form can be crossed out by the possibility of their illegal copying, modification, and distribution without regard to copyright.

The intensive development of multimedia content processing tools exacerbates the current situation, as it simplifies the process of unauthorized changes to multimedia content by third parties.

In modern educational systems based on electronic document management, without which the sustainable development of educational institutions of the Russian Federation is inconceivable, information is always presented in a compressed form, but the more sophisticated the compression methods become, the less is the opportunity to embed extraneous information. This problem can be overcome and solved by using digital watermarking techniques [1].

Digital watermarking is one of the common topics in information security and data hiding [2, 3]. To solve the task of protecting intellectual property in e-learning systems are used a technology aimed at protecting intellectual property by introducing marks in the original multimedia content to identify the author of the work.

In e-learning, some tasks allow you to solve steganography methods:

1. Copyright protection by preventing the ability to copy and duplicate multimedia content. There is the possibility of introducing a digital watermark that allows playback, prohibiting the copying and editing of multimedia information.

2. Authentication and identification. Determining the authenticity of information obtained through the network is still an important problem of e-learning, in which student knowledge is evaluated based on individual work performed and the results of distance testing.

3. Hidden annotation of documents.

III. MULTIMEDIA CONTENT PROTECTION

The main classification is the working domain, that divided into spatial and frequency domains [2]. Digital watermarks are divided into visible and invisible. Visible digital watermarks are pretty simple to remove or replace. Graphics editors such as Adobe Photoshop can be used for this. Invisible digital watermarks are data embedded in multimedia content that are not visible to the human eye.

Fig. 1. Embedding information using the Least Significant Bits method.

Digital images are characterized by significant psycho-visual redundancy [4] and are a matrix of pixels – single image elements. Image pixels are encoded with 8-bit values. The least significant bit of such an 8-bit value carries the least information. The human visual system is insensitive to small details, which are determined by changes in the least significant bit. These features of human vision are used, for example, in the development of compression algorithms for audio, images, and video. In other words, the least significant bit can be used to embed information [5]. Thus, for a full-color image, the volume of the embedded message can be more than $\frac{1}{8}$ the volume of the container.

The method of embedding data in the least significant bits, or the LSB (Least Significant Bit) method, is one of the easiest to implement, and one of the fastest watermarking methods [5]. The basic idea, according to which information is protected, is shown in Figure 1. The Least Significant Bits method is one of the earliest methods in steganography and is used for embedding in various types of multimedia content. It consists of using the sampling error that is always present in digital images [6].

The classical Least Significant Bits method does not use models of psycho-visual perception, or any estimates of the error added by the method into the container that occurs when embedding messages [5]. To increase the durability, as a rule, a secret key is used that defines the set of pixels available for embedding.

Empty container Watermarked image Distortion

Fig. 2. Results for the Least Significant Bits method.

Figure 2 shows an example of image protection using the Least Significant Bits method. The watermarked image is different from the original. Other things being equal, the larger the embedded message, the greater the distortion. Unfortunately, this method has a lot of disadvantages, one of which is low robustness against attacks in all modern e-learning systems as wide range image processing methods. The distortions added by the watermarking algorithm cannot be detected using human vision since for the watermarked image PSNR = 51.14 dB.

IV. WATERMARK EMBEDDING

Generally, a large variety of existing image coding approaches using transform-based techniques utilizing discrete cosine transform [7, 8], discrete wavelet transforms [9-11] or Karhunen-Loeve transforms to prediction-based techniques, such as CALIC [12] or LOCO-I [13].

Most e-learning systems using the standards, which based on major ISO/IEC and ITU-T standards such as JPEG [8], JPEG-LS [14], and JPEG 2000 [9]. Thus, the technique of image approximation is the main stage in the construction of a set of subsequent processing and analysis algorithms. The concept of wavelet analysis was first introduced by Meyer [15] and Malla [16] and further developed by Malla [17-18].

The most popular wavelet transform is the Haar transform [19]. Haar transform underlies many algorithms and graphics libraries. However, the basis functions of the Haar transform is not smooth, which leads to the appearance of artifacts when encoding images.

As a result, the developed e-learning system uses the method of approximation of images using Le Gall transform [20]. The image represented as a set of wavelet coefficients of

the Le Gall transform can be perform filtering operations, for example, to compress, remove noise, thresholding, and others [21]. This approach to computing a Le Gall transform has low computational complexity. An example of the decomposition of a reference image is shown in Figure 3.

Fig. 3. An example of a reference image its three-level wavelet transform

A watermark is a sequence of numbers ω_i of length K, which is embedded in the selected subset of pixels in the original image f.

The main expression for embedding information, in this case, is:

$$g(x_i, y_j) = f(x_i, y_j) \cdot (1 + \alpha \cdot \omega_i) \quad (1)$$

where α is a gain factor.

Another way to embed a watermark was proposed by I. Cox[22]:

$$g(x_i, y_j) = f(x_i, y_j) + \alpha \cdot \omega_i \quad (2)$$

M. Corvi in [23] used the additive rule of embedding.

A watermarked reference image with a gain factor $\alpha = 0.1$ is shown in Figure 4.

Fig. 4. A watermarked image, $\alpha = 0.1$

The additive method of securing multimedia content implemented in the e-learning system based on the Le Gall wavelet transform involves embedding a watermark to the low-frequency domain of the wavelet spectrum, which is a sequence of pseudorandom numbers with a normal distribution.

V. Experimental results

To study the robustness of the additive method of securing multimedia content implemented in the e-learning system based on the Le Gall wavelet transform, experiments were carried out to embedded and extract a watermark after added various deliberate distortions.

One of the serious problems of image watermarking is that adequate criteria for assessing image quality losses during embedding have not yet been found.

The digital image is a discrete field f_{ij} (matrix size $m \times n$):

$$f_{ij} = f(x_i, y_j) \quad (3)$$

Thus image$f$ – is the original image, i.e. fixed value matrix $f(x, y)$ taken at fixed points (x_i, y_j), i.e. $f(x_i, y_j)$ is the pixel value of an empty container, and $g(x_i, y_j)$ is the pixel value of a watermarked image that is the image obtained after embedding the digital watermark.

To estimate the distortion, the Mean Square Error can be used [24]:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left| f(x_i, y_j) - g(x_i, y_j) \right|^2 \quad (4)$$

It can also use the Root Mean Square metric, which is a variation of the standard deviation measure and is written as follows [6]:

$$RMS = \sqrt{\frac{1}{m \cdot n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left| f(x_i, y_j) - g(x_i, y_j) \right|^2} \quad (5)$$

According to the Root Mean Square metric, the image will be greatly corrupted when the brightness is reduced by only 5%, but the human vision will not detect this, because, for various monitors, the brightness setting changes much more. At the same time, images with noise which is a sharp change in the color of individual pixels, minor stripes, or moire will be considered almost unchanged.

To quantify the magnitude of the distortion by the digital watermarking method in the low-frequency domain of the wavelet spectrum, it is preferable to use the Peak Signal-to-Noise Ratio.

To assess the quality of the reconstructed image, a measure of the Peak Signal-to-Noise Ratio (PSNR) is also often used. It should be noted that both measures are not always in good agreement with the visually perceived error. This visual quality assessment index is generally accepted in the given subject area and is computed by the following equation:

$$PSNR = 20 \times log_{10} \frac{255}{\sqrt{\frac{1}{m \cdot n} \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} (f_{i,j} - g_{i,j})^2}}, \quad (6)$$

The Structural SIMilarity index is a methodology for measuring the similarity of two images related to full reference metrics [25]. To measure the quality of the processed image, a noiseless and original image is required. This technique was developed as a replacement for MSE and PSNR metrics that do not take into account the characteristics of human perception.

In this study, we will consider the problem of image watermarking in the frequency domain by modifying the wavelet transform coefficients. It will attack the reference images, one of which is the Lena image with a resolution of 512x512, $\alpha = 0.1$ divided into 10 areas. It should be noted that experiments were performed on other images, such as Baboon, Barbara, Pepper, Santiago, Cameramen, Elain, etc. with varying a lot of parameters in a wide range. By default, a watermark is a 32x32 pseudorandom number matrix embedded in the low-frequency domain. Let us estimate the robustness to various attacks, and also calculate the Structural Similarity Index.

For an image with an embedded watermark at $\alpha = 0.1$, shown in Figure 4, the PSNR was 37.65 dB. For $\alpha \geq 0.5$, distortions by watermarking the original image become visually perceived. PSNR of watermarked images for different gain factors is shown in Figure 5.

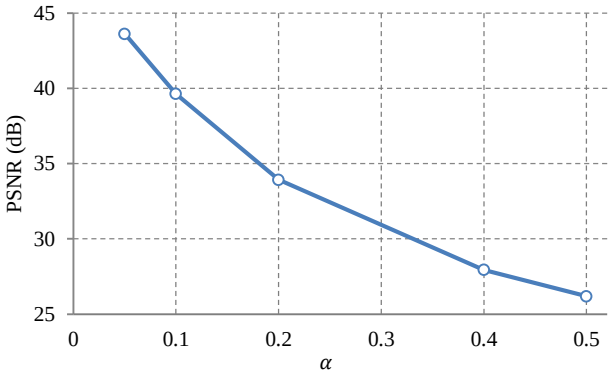

Fig. 5. PSNR of watermarked images for different gain factor

The study presents graphs of the relationship between Peak Signal-to-Noise Ratio and the degree of the attack by the mosaic and noise adding as a percentage, showing the proportion of data that has been distorted. Figure 6 and Figure 7 show that in all the above cases including those shown in the figures similar dependencies are observed.

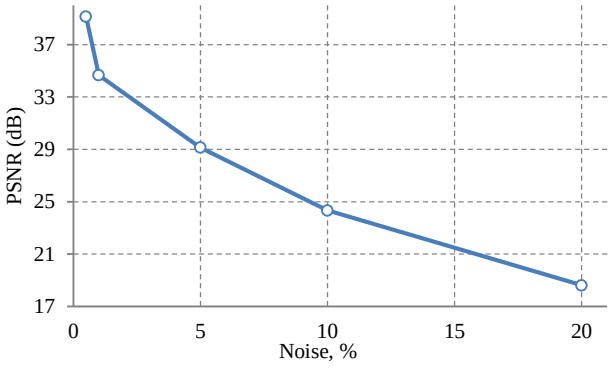

Fig. 6. PSNR of watermarked images for different noise attack

To increase robustness to various attacks, the implemented method of securing multimedia content implemented in the e-learning system proposes to embed ω_i in the coefficients of the low-frequency domain of the wavelet spectrum of the source image containing the main energy during image reconstruction using the inverse wavelet transform. Modern image compression methods use high and medium frequencies for quantization [6].

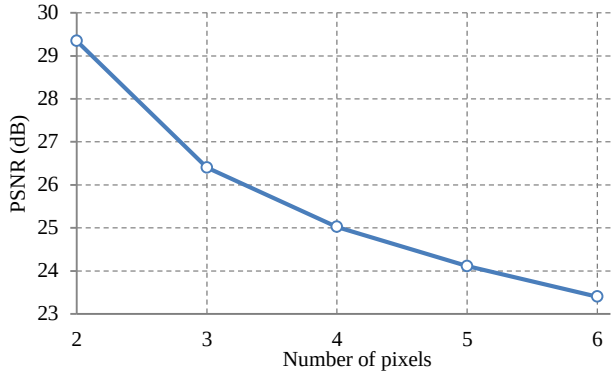

Fig. 7. PSNR of watermarked images for different mosaic attack

To reduce the added distortion, some methods use a high-frequency domain of the wavelet spectrum of the image which has a noise nature to embed ω_i.

In this study, it is proposed to control the distortion of the DC component by adding into the formula (1) the average value f_{mean} of the coefficients of the low-frequency domain: $g(x_i, y_j) = f_{mean} + (f(x_i, y_j) - f_{mean}) \cdot (1 + \alpha \cdot \omega_i)$. This allows us to reduce the distortions added into the coefficients of the low-frequency domain of the wavelet spectrum, due to which the method can be adapted for joint use with image compression methods which are already implemented in the e-learning system.

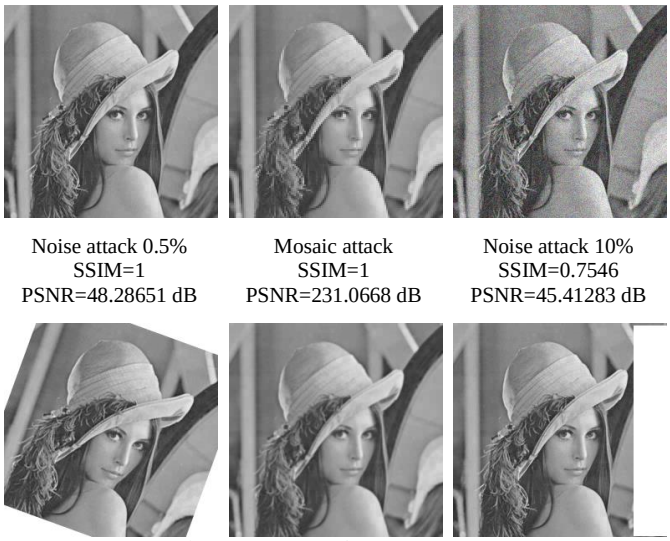

Fig. 8. The perceptual quality of the watermarked image in terms of PSNR and SSIM.

As you know, each image pixel in the RGB color model is defined by 3 channels: R, G, and B, and for a black-and-white

image, the values for each channel are equal. Image watermarking occurs by using one of some orthogonal transform and subsequent embedding of a given signature into the obtained frequency domain of the image.

Usually, this is also some kind of image, which is a company logo, a text message, a sequence of pseudorandom numbers, or even a fingerprint of the copyright owner. The embedding of a watermark is accompanied by the appearance of distortions. The total contribution of these distortions should be minimal. To assess the robustness of extracting the watermark, we will use the correlation coefficient. The perceptual quality of the watermarked image in terms of PSNR and SSIM shown in Figure 8.

As can be seen from the experimental results, the greatest value of SSIM = 1 is obtained if the method is robust against this type of attack. In this case, the embedded and extracted watermarks are completely identical. In other cases, SSIM is different from one, which indicates data corruption, manifests itself to varying degrees.

For clarity, Figures 9 and 10 show the dependences of the correlation of watermarks on the intensity of the mosaic attack and noise. The experimental results obtained show satisfactory statistics of the performance of the watermarking method based on wavelet transform.

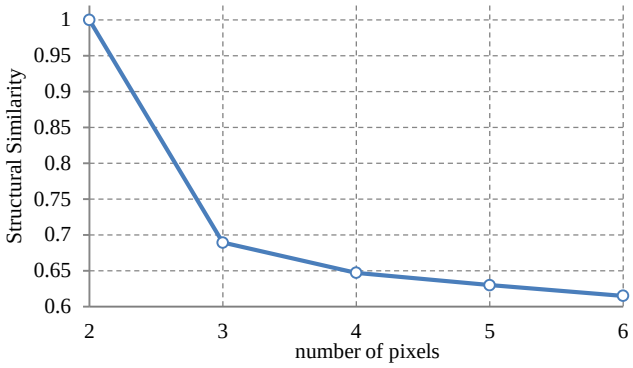

Fig. 9. SSIM of watermark for different mosaic attack

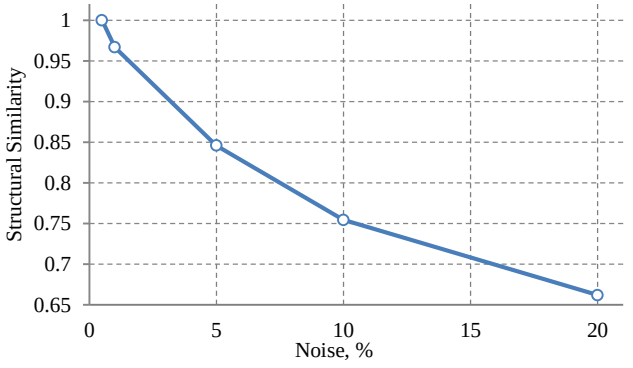

Fig. 10. SSIM of watermark for different noise attack

As can be seen from the graphs, the general view of the dependence of the correlation on the degree of attack intensity is obvious and close to the results shown in Figures 6 and 7: the higher the degree of attack, the less correlation, but the nature of the effect of various attacks can differ significantly. With an increase in the number of pixels in the mosaic from 2 to 3, the value of the correlation coefficient decreases sharply, and then the intensity of the differences is less pronounced.

VI. Conclusion

In many countries of the world, there are various restrictions on the use of cryptocurrencies, which significantly affects the development and application of information security methods in e-learning systems. The use of such methods seems extremely relevant. There is a wide class of e-learning systems in which the use of traditional methods is not preferable, because does not provide authentication of multimedia information undergoing multiple transformations. According to the experimental results and the patterns, the implemented additive method of securing multimedia content based on the Le Gall wavelet transform is more robust against multiple image attacks such as bit-plan removal, cropping, JPEG compression, histogram equalization, low-pass filtering, and noise adding than a lot of other methods and provides low distortions, and provides the required level of reliability of information extraction. Experimental results are much better than the results obtained using Haar wavelets or discrete cosine transform. It should be noted that this solution based on the wavelet transform is preferred, but not final.

References

[1] F. Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition, CRC Press, 2017.

[2] U.H. Panchal, R.A. Srivastava. A comprehensive survey on digital image watermarking techniques, Proceedings – 2015 5th International Conference on Communication Systems and Network Technologies, CSNT, pp.591-595, 2015.

[3] V.M. Potdar, H. Song, C. Elizabeth, A survey of digital image watermarking techniques, 3rd IEEE International Conference on Industrial Informatics, INDIN, pp.709-716, 2005.

[4] D.L. Donoho, Compressed sensing, IEEE Transactions on Information Theory, 52(4), pp.1289-1306, 2006.

[5] M. Khodaei, K. Faez, New Adaptive Steganographic Method Using Least Significant-Bit Substitution and Pixel-Value Differencing, Image Processing, IET 6 (6), pp.677-686, 2012.

[6] Y.Q. Shi, H. Sun, Image and Video Compression for Multimedia Engineering Fundamentals, Algorithms, and Standards, Third Edition CRC Press, 2019.

[7] W.B. Pennebaker, J.L. Mitchell, JPEG Still Image Data Compression Standard, 1st edition, Kluwer Academic Publishers, 1992.

[8] ISO/IEC 10918-1 j ITU-T Rec. T.81, Information Technology – Digital Compression and Coding of Continuous-tone Still Images, 1992.

[9] ISO/IEC 15444-1 j ITU-T Rec. T.800, Information Technology - JPEG 2000 Image Coding System: Core Coding System, 2002.

[10] I. Daubechies, The Wavelet Transform, Time-Frequency Localization and Signal Analysis, IEEE Transactions on Information Theory, vol. 36, Issue 5, pp. 961-1005, September 1990.

[11] C. K. Chui, An Introduction to Wavelets, Academic Press, NY, 1992 266 p.

[12] X. Wu, N. Memon, Context-based, adaptive, lossless image coding, IEEE Trans. Commun. 45, pp. 437-444, 1997.

[13] M.J. Weinberger, G. Seroussi, G. Sapiro, The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS, IEEE Trans. Image Process. 9, pp. 1309-1324, 2000.

[14] ISO/IEC 14495-1 j ITU-T Rec. T.87, Information Technology – Lossless and Near-lossless Compression of Continuous-tone Still Images: Baseline, 1998.

[15] Y Meyer, Ondelettes et functions splines, Seminaire EDP, Ecole Polytechnique, Paris, 1986

[16] S. Mallat, Multiresolution representation and wavelets: PhD thesis, Univ. of Pennsylvania, Philadelphia, 1988.

[17] S. Mallat, A theory of multiresolution signal decomposition: the wavelet representation, IEEE Trans. Pattern Anal. Machine Intell. 11, pp. 674-693, 1989.

[18] S. Mallat, Multiresolution approximations and wavelets orthonormal bases of $L^2(R)$, Trans. Amer. Math. Soc. 315, p. 69-87, 1989.

[19] A. Haar, Zur Theorie der orthogonalen Funktionensysteme, Math. Ann. 69, pp. 331-371, 1910.

[20] D. Gall, A. Tabiatai, Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques, Speech and Signal Processing, pp. 761-764, 1988.

[21] A.N. Zemtsov, Representation of Images using Le Gall Transform. Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie vychislitelnaja tehnika i informatika, Tomsk State University Journal of Control and Computer Science, 43, pp. 42-48, 2018.

[22] I.J. Cox, J. Kilian, T. Leighton, T.G. Shamoon, Secure spread spectrum watermarking for multimedia, Proceedings of the IEEE International Conference on Image Processing, Vol. 6, pp. 1673-1687, 1997.

[23] Corvi M., Nicchiotti G. Wavelet-based image watermarking for copyright protection, Scandinavian Conference on Image Analysis, pp. 157-163, 1997.

[24] D.R. Newlin, C.C. Seldev, Medical image denoising using different techniques, International Journal of Scientific and Technology Research 9(3), pp. 1061-1066, 2020.

[25] Y. Fang, K. Zeng, Z. Wang, Z. Fang, C.W. Lin, Objective quality assessment for image retargeting based on structural similarity, IEEE Journal on Emerging and Selected Topics in Circuits and Systems, Vol. 4, pp. 95-105, 2014.