Paper

SVD Audio Watermarking: A Tool to Enhance the Security of Image Transmission over ZigBee Networks

Mohsen A. M. El-Bendary[a], Atef Abou El-Azm[b], Nawal El-Fishawy[b], Farid Shawki[b], Mostafa A. R. El-Tokhy[a], Fathi E. Abd El-Samie[b], and H. B. Kazemian[c]

[a] Department of Communication Technology, Faculty of Industrial Education, Helwan University, Egypt
[b] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt
[c] Intelligent Systems Research Centre, Faculty of Computing, London Metropolitan University, UK

Abstract—The security is important issue in wireless networks. This paper discusses audio watermarking as a tool to improve the security of image communication over the IEEE 802.15.4 ZigBee network. The adopted watermarking method implements the Singular-Value Decomposition (SVD) mathematical technique. This method is based on embedding a chaotic encrypted image in the Singular Values (SVs) of the audio signal after transforming it into a 2-D format. The objective of chaotic encryption is to enhance the level of security and resist different attacks. Experimental results show that the SVD audio watermarking method maintains the high quality of the audio signals and that the watermark extraction and decryption are possible even in the presence of attacks over the ZigBee network.

Keywords—audio watermarking, copyright protection, IEEE 802.15.4, SVD.

1. Introduction

With the increase in utilization of wireless devices, especially Bluetooth and ZigBee devices, the need for data security has evolved. Generally, wireless network security is a problem, because the transmitted data can be easily overheard by eavesdropping devices if no security strategies have been adopted. The choice of security levels is based on the application [1]. ZigBee has a set of security services implementing the Advanced Encryption Standard (AES). In this paper, we use digital audio watermarking to enhance the security of image communication over ZigBee networks.

Digital watermarking has found several applications in image, video, and audio communication. Watermarking is the art of embedding a piece of information in a cover signal. It can achieve several objectives such as information hiding, copyright protection, fingerprinting, and authentication [2]. Several algorithms have been proposed for watermarking, especially for image and video watermarking [3]–[5]. Some of these algorithms are designed for the efficient embedding and detection of the watermark, but most of them aim at the successful extraction of the embedded watermark. On the other hand, most of the audio watermarking algorithms are designed to achieve an efficient detection of the watermark without extracting meaningful information from the watermarked audio signal [6]–[7].

There is a need for a robust audio watermarking method with a higher degree of security, which can be achieved by embedding encrypted images in audio signals. In this paper, the chaotic Baker map is used for the encryption of the watermark image [8]. Then, the watermark is embedded in the audio signal using the SVD mathematical technique. The audio signal is first transformed into a 2-D format and the SVs of the resulting matrix are used for watermark embedding. The watermarked audio signal is then transmitted over the ZigBee network [9].

Embedding encrypted images in audio signals achieves two levels of security; the level of encryption and the level of watermarking. Encryption can be performed with either diffusion or permutation-based algorithms. Diffusion-based algorithms are very sensitive to noise, while permutation based algorithms are more immune to noise. That is why the adopted encryption scheme in this paper is based on the chaotic Baker map, which is permutation-based.

The paper is organized as follows. In Section 2, the IEEE 802.15.4 ZigBee standard is discussed. Section 3 explains the SVD audio watermarking method. In Section 4, chaotic encryption is briefly discussed. The simulation results are introduced in Section 5. Finally, the concluding remarks are given in Section 6.

2. ZigBee Standard

IEEE 802.15.4 is a Low-Rate Wireless Personal Area Network (LR-WPAN) standard used for providing simple and low-cost communication networks. LR-WPANs are intended for short-range operation, and use little or no infrastructure. This standard focuses on applications with limited power and relaxed throughput requirements, with the main objectives being ease of installation and reliable data transfer. This allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices. Low power consumption can be achieved by allowing a device to sleep, only waking into active mode for brief periods. Enabling such low-duty-cycle operation is at the heart of the IEEE 802.15.4 standard [10]. The ZigBee specification document is short, allowing a small and simple stack, in contrast to other wireless standards such as Bluetooth [11].

The IEEE 802.15.4 standard conforms to the established regulations in Europe, Japan, Canada and the United States, and defines two physical (PHY) layers; the 2.4-GHz and the 868/915-MHz band PHY layers. Although the PHY layer chosen depends on local regulations and user preference, for the purposes of this document only the higher data-rate, worldwide, unlicensed 2.4-GHz band will be considered. Sixteen channels are available in the 2.4-GHz band, numbered 11 to 26, each with a bandwidth of 2 MHz and a channel separation of 5 MHz. LR-WPAN output powers are around 0 dBm and typically operate within a 50-m range [12].

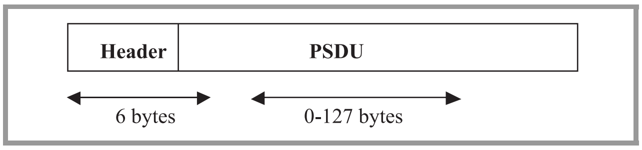


Fig. 1. ZigBee packet format.

The structure of the ZigBee packet is shown in Fig. 1. The header contains three fields; a preamble of 32 bits for synchronization, a packet delimiter of 8 bits, and a physical header of 8 bits. The Physical Service Data Unit (PSDU) field is the data field with 0 to 1016 bits. ZigBee uses an error detection/retransmission technique through a Cyclic-Redundancy Check (CRC) scheme. For image communication over the ZigBee network, data fragmentation into packets is implemented.

3. SVD Audio Watermarking

The SVD mathematical technique provides an elegant way for extracting algebraic features from a 2-D matrix. The main properties of the matrix of SVs can be exploited in audio watermarking. When a small perturbation happens to the original data matrix, no large variations occur in the matrix of SVs, which makes this technique robust to attacks [13]-[15].

The steps of the SVD audio watermark embedding algorithm are summarized as follows:

1. The 1-D audio signal is transformed into a 2-D matrix ($\mathbf{A}$ matrix).
2. The SVD is performed on the $\mathbf{A}$ matrix.
$$\mathbf{A} = \mathbf{USV}^{\mathrm{T}}. \tag{1}$$
where: $\mathbf{U}$ and $\mathbf{V}$ are orthogonal matrices such that $\mathbf{U}^{\mathrm{T}}\mathbf{U} = \mathbf{I}$, and $\mathbf{V}^{\mathrm{T}}\mathbf{V} = \mathbf{I}$, $\mathbf{S} = diag(\sigma_1, \ldots, \sigma_P)$, where $\sigma \geq \sigma_2 \geq \ldots \geq \sigma_P \geq 0$ are the SVs of $\mathbf{A}$, the columns of $\mathbf{U}$ are called the left singular vectors of $\mathbf{A}$, and the columns of $\mathbf{V}$ are called the right singular vectors of $\mathbf{A}$.
3. The chaotic encrypted watermark ($\mathbf{W}$ matrix) is added to the SVs of the original matrix.
$$\mathbf{D} = \mathbf{S} + k\mathbf{W}. \tag{2}$$
A small value of k of about 0.01 is required to keep the audio signal undistorted.
4. The SVD is performed on the new modified matrix ($\mathbf{D}$ matrix).
$$\mathbf{D} = \mathbf{U}_{\mathrm{w}}\mathbf{S}_{\mathrm{w}}\mathbf{V}_{\mathrm{w}}^{\mathrm{T}}. \tag{3}$$
5. The watermarked signal in 2-D format ($\mathbf{A}_w$ matrix) is obtained using the modified matrix of SVs ($\mathbf{S}_w$ matrix).
$$\mathbf{A}_{\mathrm{w}} = \mathbf{US}_{\mathrm{w}}\mathbf{V}^{\mathrm{T}}. \tag{4}$$
6. The 2-D $\mathbf{A}_{\mathrm{w}}$ matrix is transformed again into a 1-D audio signal.

To extract the possibly corrupted watermark from the possibly distorted watermarked audio signal, given $\mathbf{U}_{\mathrm{w}}$, $\mathbf{S}$, $\mathbf{V}_{\mathrm{w}}$ matrices, and the possibly distorted audio signal, the above steps are reversed as follows:

1. The 1-D audio signal is transformed into a 2-D matrix $\mathbf{A}_{\mathrm{w}}^*$. The $*$ refers to the corruption due to attacks.
2. The SVD is performed on the possibly distorted watermarked image ($\mathbf{A}_{\mathrm{w}}^*$ matrix).
$$\mathbf{A}_{\mathrm{w}}^* = \mathbf{U}^*\mathbf{S}_{\mathrm{w}}^*\mathbf{V}^{*\mathrm{T}}. \tag{5}$$
3. The matrix that includes the watermark is computed.
$$\mathbf{D}^* = \mathbf{U}_{\mathrm{w}}\mathbf{S}_{\mathrm{w}}^*\mathbf{V}_{\mathrm{w}}^{\mathrm{T}}. \tag{6}$$
4. The possibly corrupted encrypted watermark is obtained.
$$\mathbf{W}^* = (\mathbf{D}^* - \mathbf{S})/k. \tag{7}$$
5. The obtained matrix $\mathbf{W}^*$ is decrypted.
6. The correlation coefficient between the decrypted matrix and the original watermark is estimated. If this coefficient is higher than a certain threshold, the watermark is present.

4. Chaotic Encryption

Chaotic encryption of the watermark image is performed using the chaotic Baker map. The Baker map is a chaotic map that generates a permuted version of a square matrix [16]. In its discretized form, the Baker map is an efficient tool to randomize a square matrix of data. The discretized map can be represented for an $R \times R$ matrix as follows:

$$B(r_1, r_2) = \left[\frac{R}{n_i}(r_1 - R_i) + r_2 \bmod \left(\frac{R}{n_i}\right), \frac{n_i}{R}\left(r_2 - r_2 \bmod \left(\frac{R}{n_i}\right)\right) + R_i\right], \tag{8}$$

where $B(r_1, r_2)$ are the new indices of the data item at (r_1, r_2), $R_i \leq r_1 \leq R_i + n_i$, $0 < r_2 < R$, and $R_i = n_1 + n_2 + \ldots + n_i$.

In steps, the chaotic encryption is performed as follows:

1. An $R \times R$ square matrix is divided into R rectangles of width n_i and number of elements R.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from left to right beginning with upper rectangles then lower ones.
3. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

Figure 2 shows an example of the chaotic encryption of an 8×8 square matrix (i.e. $R = 8$). The secret key is $S_{key} = [n_1, n_2, n_3] = [2, 4, 2]$.

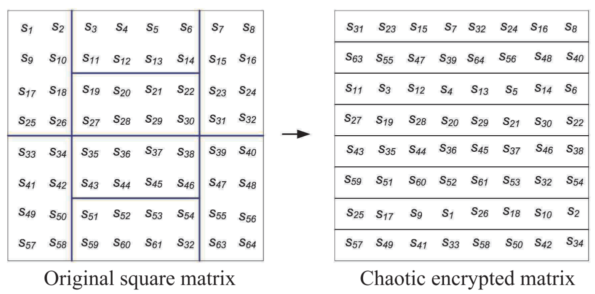


Fig. 2. Chaotic encryption of an 8×8 matrix.

5. Simulation Results

In this section, the computer simulation results are presented. The effectiveness of the SVD audio watermarking method is studied for the transmission of watermarked audio signals over fading channels. Firstly, an uncorrelated block-fading channel is considered. It is a slow and frequency non-selective channel, where symbols in a block undergo a constant fading effect. This means that the Doppler spread is equal to zero ($f_d = 0$) [17]. Also, the correlated Rayleigh fading channel is considered. The channel model utilized is the Jakes' model [18]. The assumed mobile ZigBee device velocity (v) is 10 miles/hour, and the carrier frequency is 2.46 GHz. The Doppler spread is $f_d = 366$ Hz. Both the logo and the cameraman images are used in the simulation experiments.

The chaotic Baker map is used to encrypt the watermark image. The encrypted image is then used as a watermark to be embedded in the Handel signal available in Matlab

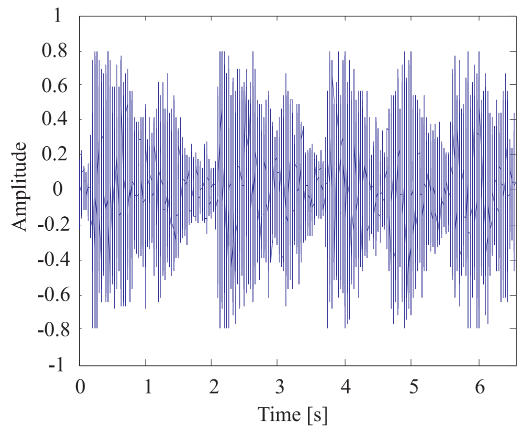


Fig. 3. Waveform of the Handel audio signal.

and shown in Fig. 3. This signal is transmitted over the ZigBee network at different signal-to-noise ratios (SNRs). In all our experiments, the correlation coefficient between the original and decrypted images (c_r) is used to measure the closeness of the decrypted watermark to the original one. Figures 4 and 5 show the original logo and cameraman images, respectively, with their encrypted versions.

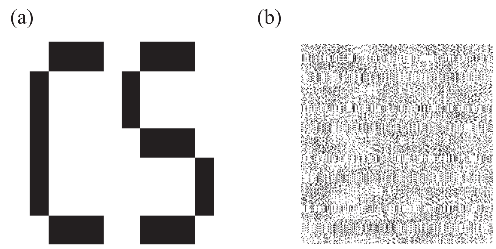


Fig. 4. Logo image: (a) original image; (b) encrypted version.

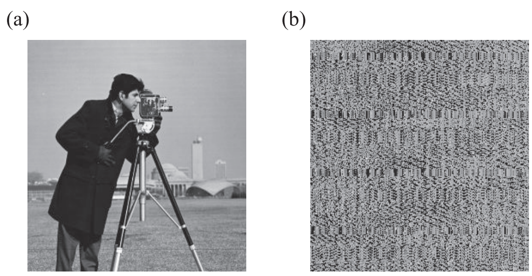


Fig. 5. Cameraman image: (a) original image; (b) encrypted version.

In the first simulation experiment, the logo image is used as a watermark. The SVD audio watermarking method has been used for watermark embedding without encryption. The watermarked audio signal has been transmitted over an uncorrelated fading channel and the results are shown in Fig. 6 at $SNR = 20$ dB. It is clear from these results that the SVD audio watermarking does not degrade the quality of the watermarked audio signal. It is also clear that

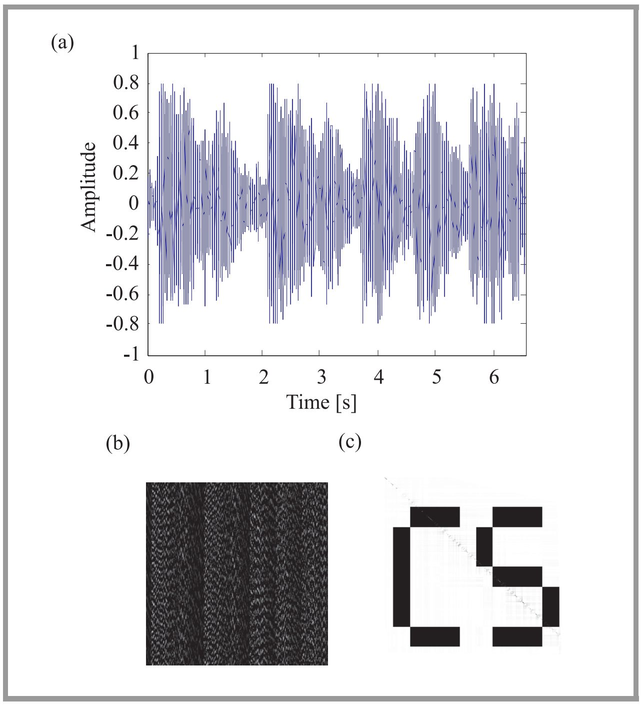


Fig. 6. Transmission of the watermarked audio signal over an uncorrelated fading channel at $SNR = 20$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted logo image, $c_r = 0.41$.

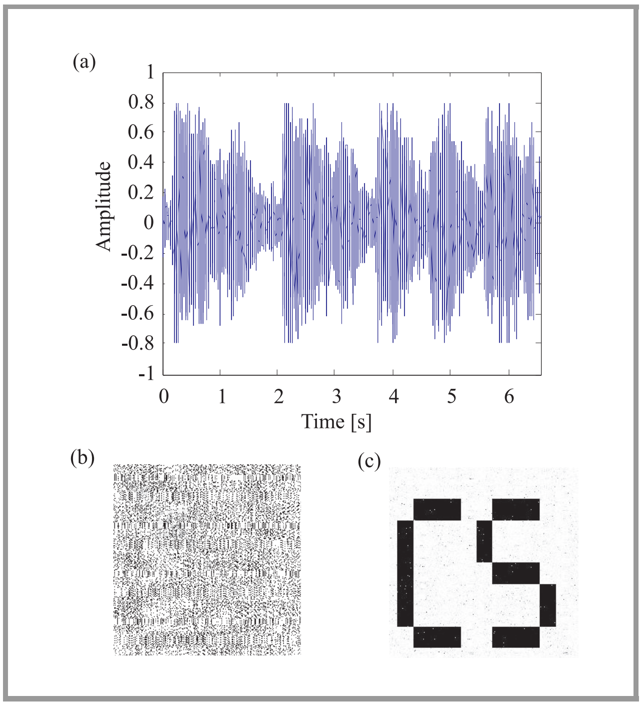


Fig. 8. Transmission of the watermarked audio signal with an encrypted watermark over an uncorrelated fading channel at $SNR = 20$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted logo image, $c_r = 0.7$.

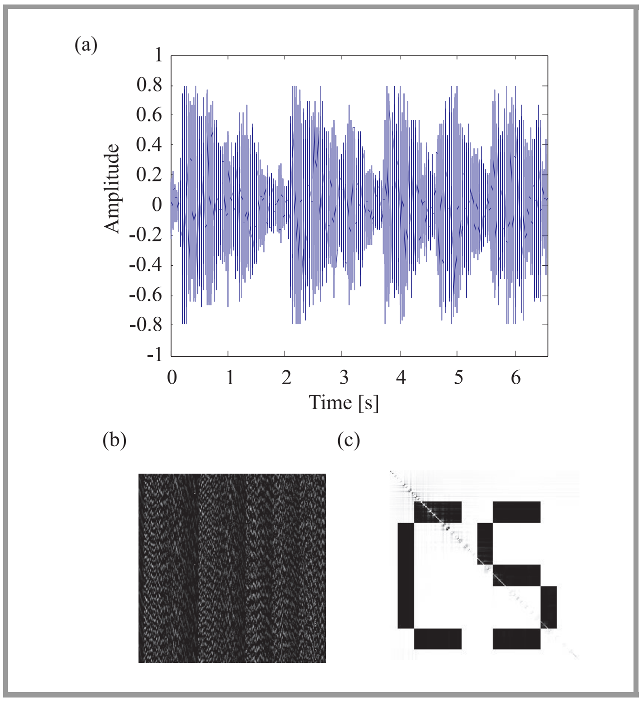


Fig. 7. Transmission of the watermarked audio signal over an uncorrelated fading channel at $SNR = 30$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted logo image, $c_r = 0.86$.

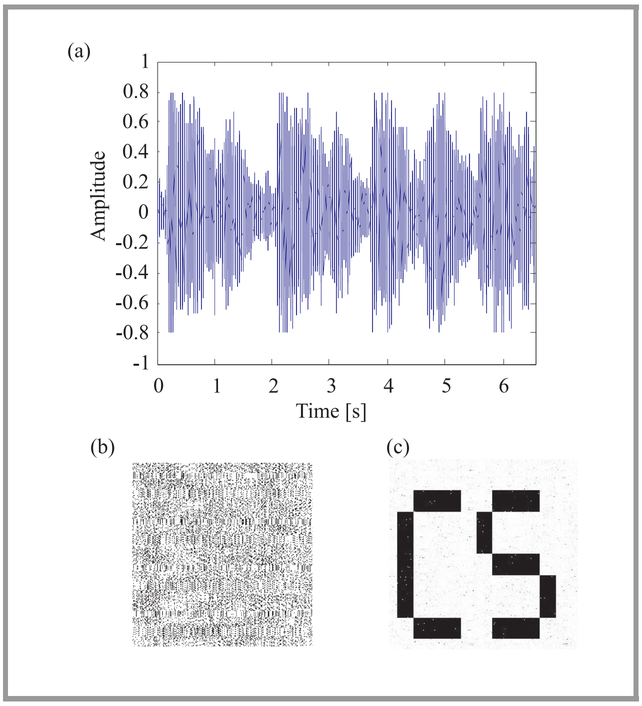


Fig. 9. Transmission of the watermarked audio signal with an encrypted watermark over an uncorrelated fading channel at $SNR = 30$ dB: (a) received audio signal; (b) the watermarked signal; (c) the extracted logo image, $c_r = 0.95$.

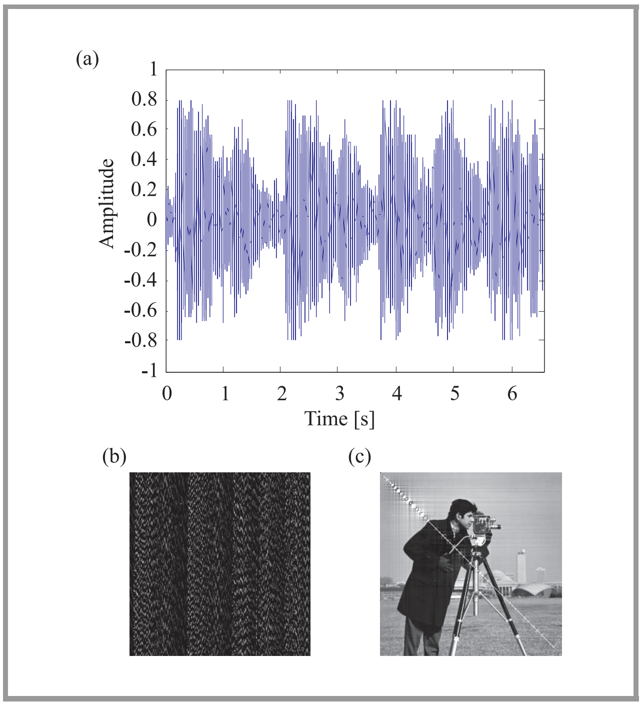


Fig. 10. Transmission of the watermarked audio signal over an uncorrelated fading channel at $SNR = 20$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted cameraman image, $c_r = 0.31$.

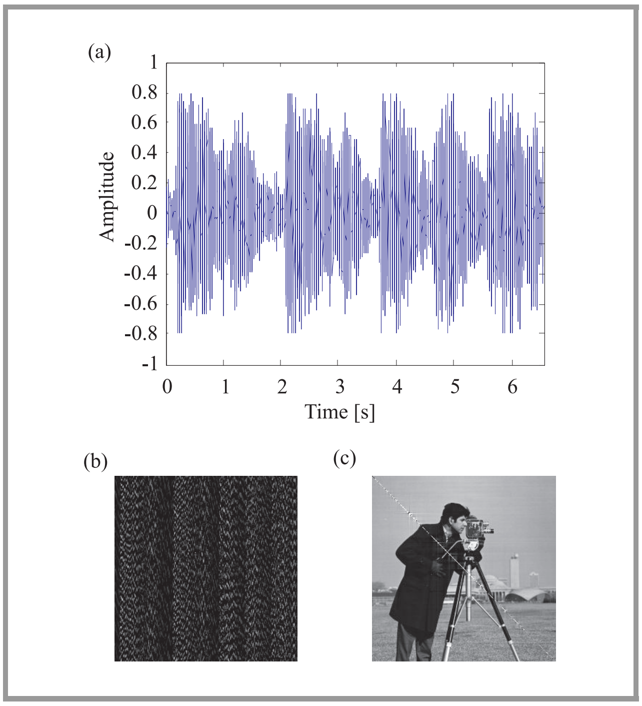


Fig. 11. Transmission of the watermarked audio signal over an uncorrelated fading channel at $SNR = 30$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted cameraman image, $c_r = 0.92$.

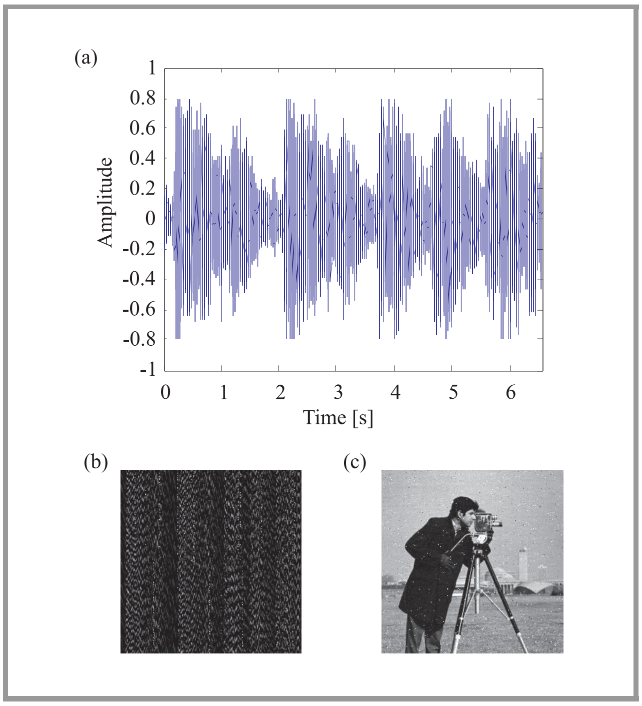


Fig. 12. Transmission of the watermarked audio signal with an encrypted watermark over an uncorrelated fading channel at $SNR = 20$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted cameraman image, $c_r = 0.33$.

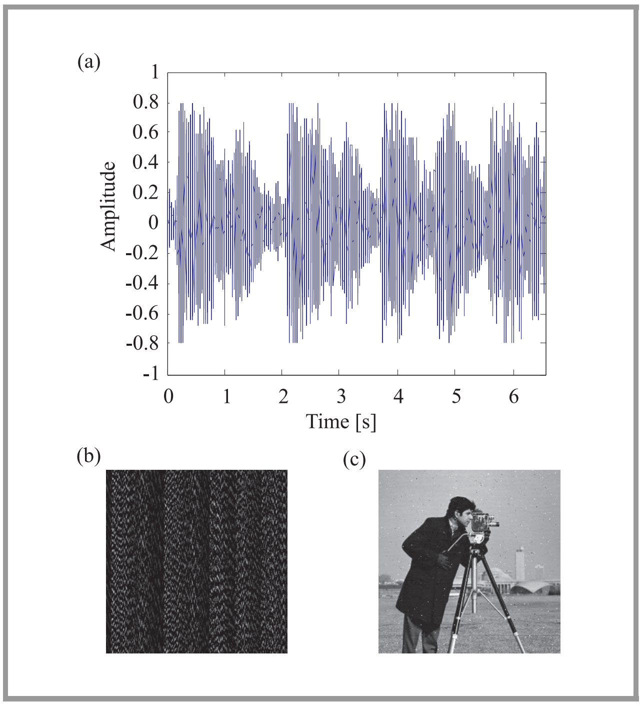


Fig. 13. Transmission of the watermarked audio signal with an encrypted watermark over an uncorrelated fading channel at $SNR = 30$ dB: (a) received audio signal; (b) the watermarked matrix; (c) the extracted cameraman image, $c_r = 0.96$.

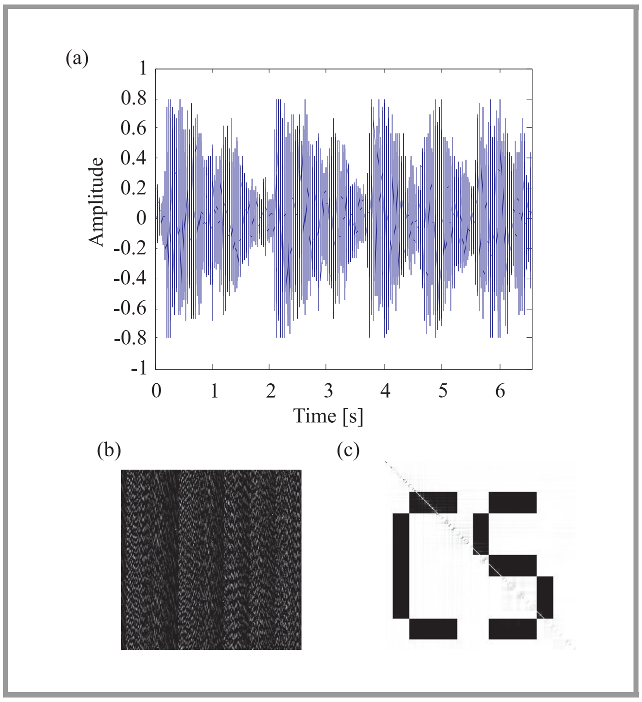


Fig. 14. Transmission of the watermarked audio signal over a correlated fading channel at $SNR = 25$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted logo image, $c_r = 0.72$.

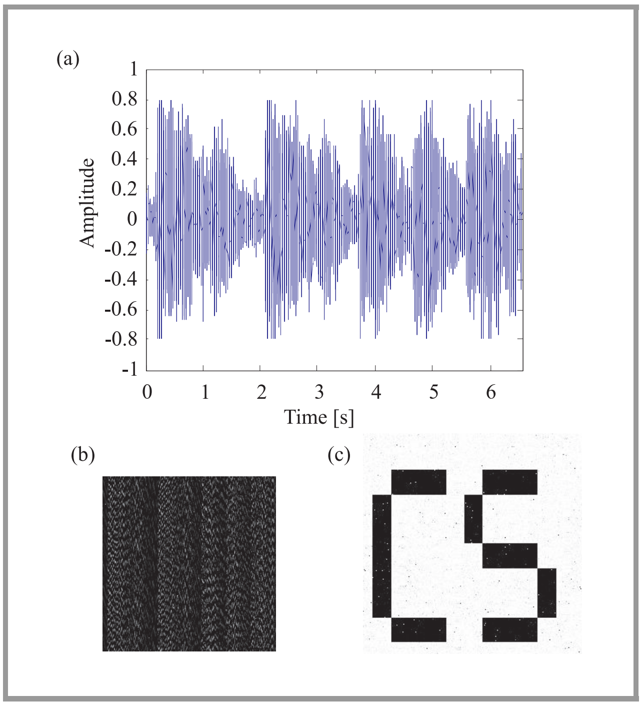


Fig. 15. Transmission of the watermarked audio signal with an encrypted watermark over a correlated fading channel at $SNR = 25$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted logo image, $c_r = 0.75$.

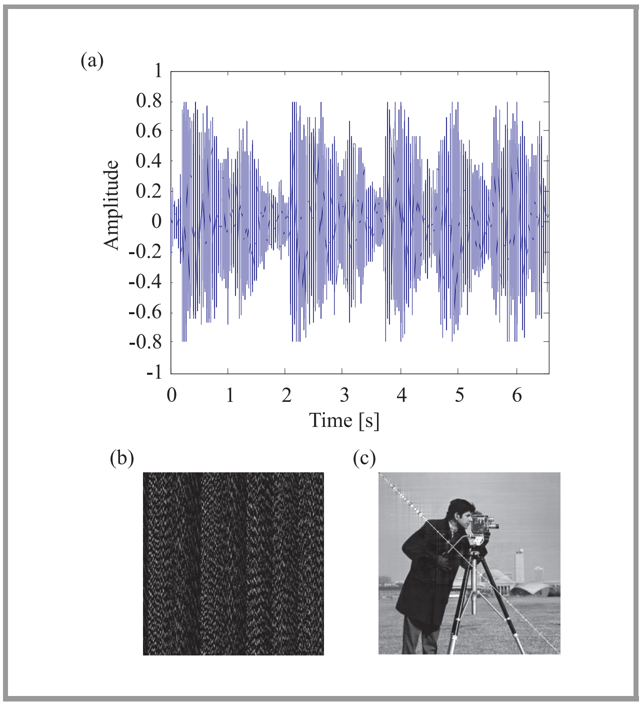


Fig. 16. Transmission of the watermarked audio signal over a correlated fading channel at $SNR = 25$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted cameraman image, $c_r = 0.5$.

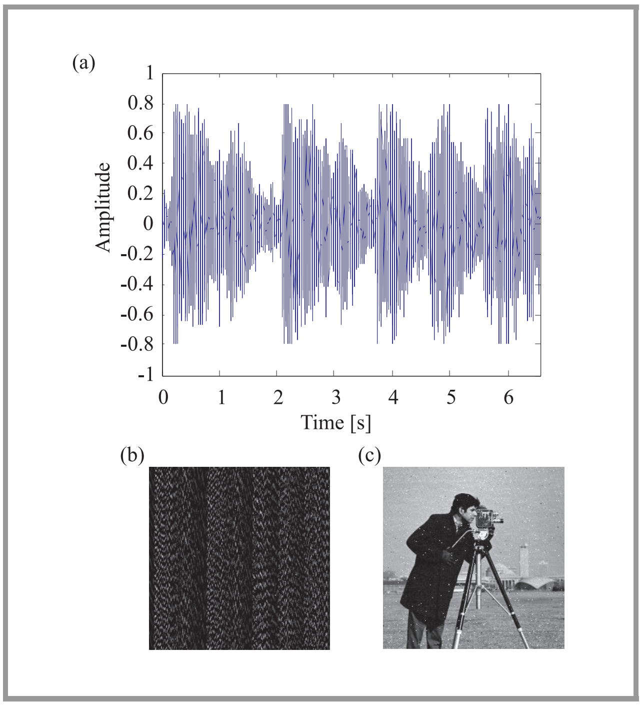


Fig. 17. Transmission of the watermarked audio signal with an encrypted watermark over an correlated fading channel at $SNR = 25$ dB: (a) received audio signal; (b) 2-D watermarked matrix; (c) the extracted cameraman image, $c_r = 0.56$.

the watermark has been reconstructed with an acceptable correlation coefficient. A similar experiment has been carried out at $SNR = 30$ dB. The results of this experiment are given in Fig. 7. As shown in these results the received audio signal and the extracted image are enhanced with the increase of the channel SNR.

Similar experiments have been carried out with encrypted watermarks. Figures 8 and 9 show the results of these experiments at $SNR = 20$ dB, and 30 dB, respectively. These results reveal that encryption enhances the quality of the extracted watermark.

In the following experiments, the cameraman image is used as the watermark. The cameraman watermark has been transmitted in the audio signal over an uncorrelated fading channel without encryption at $SNR = 20$ dB and 30 dB. The results of these experiments are given in Figs. 10 and 11, respectively.

The encrypted cameraman image has also been used in another experiment as a watermark. The results of this experiment over an uncorrelated fading channel are given in Figs. 12 and 13 at $SNR = 20$ dB and 30 dB, respectively.

After studying the performance of the SVD audio watermarking technique with the ZigBee network over an uncorrelated fading channel, the following experiments will study the performance of this method over a correlated fading channel with the Jakes' model. The results of these experiments at $SNR = 25$ dB are shown in Figs. 14 to 17.

All previous results reveal the robustness of the SVD audio watermarking method in the transmission of images over the ZigBee network. Also, the results reveal the effectiveness of chaotic encryption to increase the security and to improve the performance of ZigBee networks in image communication.

6. Conclusions

This paper presented an efficient method for image communication with ZigBee networks. This method is based on data hiding with SVD audio watermarking. Experimental results have proved that watermark embedding with the SVD audio watermarking method does not deteriorate the audio signals. It is clear through experiments that the chaotic encryption enhances the performance of the ZigBee network and increases the level of security.

References

[1] G. Pekhteryev, Z. Sahinoglu, P. Orlik, and G. Bhatti, "Image transmission over IEEE 802.15.4 and ZigBee Networks", in *Proc. IEEE ISCAS*, Kobe, Japan, May 2005.

[2] B. Macq, J. Dittmann, and E. J. Delp, "Benchmarking of image watermarking algorithms for digital rights management", *Proc. of the IEEE*, vol. 92, no. 6, pp. 971–984, 2004.

[3] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization", *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 822–831, 2005.

[4] H. S. Kim and H. K. Lee, "Invariant image watermark using zernike moments", *IEEE Trans. Circ. Syst. Video Technol.*, vol. 13, no. 8, pp. 766–775, 2003.

[5] W. C. Chu, " DCT-based image watermarking using subsampling", *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 34–38, 2003.

[6] L. Ghouti, A. Bouridane, M. K. Ibrahim, and Said Boussakta, "Digital image watermarking using balanced multiwavelets", *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1519–1536, 2006.

[7] S. Xiang and J. Huang, "Histogram-based audio watermarking against time-scale modification and cropping attacks", *IEEE Trans. Multimedia*, vol. 9, no. 7, pp. 1357–1372, 2007.

[8] Z. Liu and A. Inoue, "Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences", *IEEE Trans. Circ. Systems Video Technol.*, vol. 13, no. 8, pp. 801–812, 2003.

[9] A. N. Lemma, J. Aprea, W. Oomen, and L. V. de Kerkhof, "A temporal domain audio watermarking technique", *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1088–1097, 2003.

[10] M. A. M. El-Bendary, A. E. Abou-El-Azzm, N. A. El-Fishawy, M. El-Tokhy, F. Shawki, F. E. Abd-El-Samie, and H. B. Kazemian, "An efficient chaotic interleaver for image transmission over IEEE 802.15.4 Zigbee network", *J. Telecom. Inform. Technol. JTIT*, vol. 2, no. 1, pp. 67–73, 2011.

[11] Q. He, Q. Qi, Y. Zhao, W. Huang, anf Q. Huang, "The application of chaotic encryption in industrial control based on ZigBee wireless network", in *Proc. Int. Symp. Systems Control Aerosp. Astronaut. ISSCAA 2008*, Shenzhen, China, 2008.

[12] M. Ise, Y. Ogasahara, K. Watanabe, M. Hatanaka, T. Onoye, H. Niwamoto, I. Keshi, and I. Shirakawa, "Design and implementation of home network protocol for appliance control based on IEEE 802.15.4", *International J. Comput. Sci. Netw. Secur.*, vol. 7 no. 7, July 2007.

[13] B. P. Lathi, *Modern Digital and Analog Communication Systems*. 2nd edition. Philadelphia: Holt, Rinehart and Winston, 1989.

[14] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership", *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, March 2002.

[15] X. Sun, J. Liu, J. Sun, Q. Zhang and W. Ji, " A robust image watermarking scheme based-on the relationship of SVD", in *Proc. Int. Conf. Intelligent Inf. Hiding and Multimedia Sig. Process.*, Harbin, China, 2008.

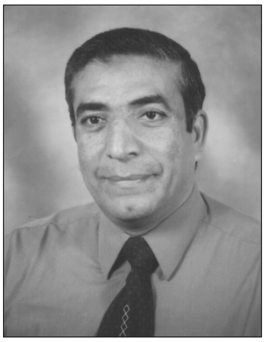
[16] X. Zhu, J. Zhao and H. Xu, "A digital watermarking algorithm and implementation based on improved SVD", in *Proc. 18th Int. Conf. Pattern Recognition ICPR'06*, Hong Kong, China, 2006.

[17] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley, 1975.

[18] J. Aldrich, "Correlations genuine and spurious in Pearson and Yule", *Statist. Sci.*, vol. 10, no. 4, pp. 364–376, 1995.

Mohsen A. M. Mohamed El-Bendary received his B.Sc. in 1998, M.Sc. in 2008, all in Communication Engineering, from Menoufia University, Faculty of Electronic Engineering. He is now a lecturer assistant and Ph.D. student. His research interests cover wireless networks, wireless technology, channel coding, QoS over

Bluetooth system and Wireless Sensor Network (WSN), and security systems which use wireless technology, such as fire alarm and access control systems.
E-mail: mohsenbendary@yahoo.com
Faculty of Industrial Education
Department of Communication Technology
Helwan University, Egypt



Atef Abou El-Azm was born in 1954, Egypt. He has the B.Sc. in Electronic Engineering and M.Sc. in Antennas from Faculty of Electronic Engineering, Menofia University in 1977 and 1984, respectively. He has the Ph.D. in Communications from Warsaw University of Technology, Poland, in 1990. His research is in the area of digital communications, with special emphasis on coding theory, information theory, error control coding, and coded modulation. Topics of current interest include the use of convolutional, trellis codes and turbo codes in the development of coding standards for high speed data modems, digital satellite communication, and deep space channels. He is the author of many papers in the field of line codes, channel codes and signal processing.
E-mail: abouelazm_atef@yahoo.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

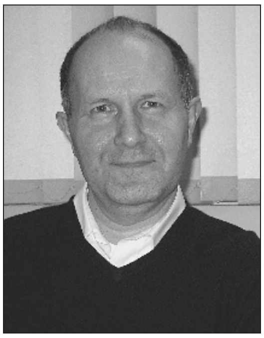
Nawal El-Fishawy received the Ph.D. degree in Mobile Communications from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Now she is the head of Computer Science and Engineering Department, Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms.
E-mail: nelfishawy@hotmail.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

Farid Shawki M. Al-Hosarey received the B.Sc. (Hons), M.Sc., and Ph.D. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1995, 2000 and 2007, respectively. In 1995 and 2000, he worked as a demonstrator and assistant lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications since 2008. His current research areas of interest include channel coding, mobile communication systems, MIMO systems, and implementation of digital communications systems using FPGA.
E-mail: farid_shawki@yahoo.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

Mostafa A. R. El-Tokhy was born in Kaluobia, Egypt, in 1970. He received his B.Sc. degree from Zagazig University, Banha branch, Egypt, and M.Sc. degree from Technical University, Eindhoven, The Netherlands in 1993 and 1998, respectively. He received his Ph.D. degree from Osaka University, Osaka, Japan in 2003. Presently, he is an Assistant Professor of Electronics Engineering at Industrial Education College, Higher Ministry of Education, Cairo Egypt. His current research interests are high performance digital circuits and analog circuits. He is a member of the IEEE.
E-mail: mostafaeltokhy@hotmail.com
Faculty of Industrial Education
Department of Communication Technology
Helwan University, Egypt

Fathi E. Abd El-Samie received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He is a co-author of about 130 papers in national and international conference proceedings and journals. He has received the most cited paper award from digital signal processing journal for 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, superresolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.

E-mail: fathi_sayed@yahoo.com
Faculty of Electronic Engineering
Department of Electronics
and Electrical Communications
Menoufia University
Menouf, 32952, Egypt



H. B. Kazemian received the B.Sc. in Engineering from Oxford Brookes University, UK, the M.Sc. in control systems engineering from the University of East London, UK, and the Ph.D. in learning fuzzy controllers from Queen Mary University of London, UK, in 1985, 1987 and 1998, respectively. He is currently a Full Professor at London Metropolitan University, UK. His research interests include fuzzy and neuro-fuzzy control of networks, 2.4 GHz frequency bands, ATM, video streaming and rate control. He is a senior member of the IEEE, IET, and Chartered Engineer, UK.

E-mail: h.kazemian@londonmet.ac.uk
Intelligent Systems Research Centre
Faculty of Computing, London Metropolitan University
London, UK