Novel Technique for Improving Bluetooth Networks Security Through SVD-Based Audio Watermarking

A. E. Abo. Elazzm, N. A. El-Fishawy. F. El-Sayed
Faculty of Electronic Engineering
Menofia University
Menof, Egypt
Fathi_sayed@yahoo.com

M. A. M. El-Bendary, M. El-Tokhy
Faculty of Industrial Education
Helwan university
Cairo, Egypt
mohsenbendary@yahoo.com

Abstract—**In this paper, we try to improve the security of image transmission over IEEE 802.15.1 Bluetooth networks. We propose a new approach for audio watermarking using the singular value decomposition (SVD) mathematical technique. This approach is based on embedding the encrypted image in the singular values of the audio signal after transforming it into a 2-D format. After watermark embedding, the audio signal is transformed again into a 1-D format. The 1-D audio signal is segmented to Bluetooth packet payload length. This leads to the needs of fragmenting of the image into small fragments. At the receiver the segments are recollected to construct the watermark signal. The final step is extracting the image. Experimental results show that the proposed audio watermarking approach maintains the high quality of the audio signal and that the watermark extraction and decryption are possible.**

Keywords-Audio Watermarking, IEEE 802.15.1 (Bluetooth Technology), SVD, Fading channel, Copyright Protection.

I. INTRODUCTION

With increasing utilization of wireless devices, especially Bluetooth and Bluetooth devices, the need of security of data has increased. In this paper, we use digital watermarking technique to enhance the security over Bluetooth networks. Because of using this wireless technology for transmitting very important data or images which must be secured (for example, medical applications), we propose this technique [1].

Digital Watermarking has found many applications in image, video and audio transmission. Watermarking is the art of embedding a piece of information in a cover signal. Watermarking 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 approach 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 [8-9]. Then, the watermark is embedded in the audio signal using the SVD mathematical technique. The audio signal is transformed into a 2-D format and the singular values (SVs) of the resulting 2-D matrix are used for watermark embedding.

The paper is organized as follows. In section II, IEEE 802.15.1 Bluetooth system is discussed. Section III explains the proposed SVD-based audio watermarking approach. In section IV, the chaotic encryption is briefly discussed. In section V the proposed algorithm with Bluetooth is discussed. In section VI, The simulation results are introduced. Finally, the paper is concluded in section VII.

II. BLUETOOTH SYSTEM

IEEE 802.15.1 is a short-range wireless communication standard defined as Wireless Personal Area Network (WPAN) standard [10] aimed at providing simple, low-cost communication networks. To counteract these limitations Bluetooth is designed to be light and portable. It can be embedded to take the riggers of physical knocks and shocks. It includes standards and protocols to make it mobile, robust, reliable and not limited to one manufacturer.

Bluetooth has three different modes of security. Each Bluetooth device can operate in one mode only at a time. These three modes are the following: security mode 1- non-secure mode, security mode 2- service-level enforced security mode, and security mode 3- link-level enforced security mode.

In security mode 1, there is not any security procedure. In this mode the security functionality such as authentication and encryption is bypassed. In security mode 2, the security procedures are initiated after the connection establishment at Logical Link Control and Adaptation Protocol (L2CAP). In security mode 3, it is the link-level security mode, a Bluetooth device initiate the security procedure before the channel is established [11-12].

III. THE PROPOSED SVD AUDIO WATERMARKING APPROACH

In this section, the proposed approach is presented. The SVD algorithm has been previously exploited in image watermarking [13-15]. In this paper, this idea is extended into 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 the 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 singular values, which makes this technique robust against attacks [15]. In our simulation, we assume the side information is error free.

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

The 1- D audio signal is transformed into a 2-D matrix (A matrix).

The SVD is performed on the A matrix.

$$A = USV^T \tag{1}$$

The chaotic encrypted watermark (W matrix) is added to the SVs of the original matrix.

$$D = S + KW \tag{2}$$

A small value of K of about 0.01 is required to keep the audio signal undistorted.

The SVD is performed on the new modified matrix (D matrix).

$$D = U_w S_w V_w^T \tag{3}$$

The watermarked signal in 2-D format (A_w matrix) is obtained using the modified matrix of SVs (S_w matrix).

$$A_w = US_w V^T \tag{4}$$

6. The 2-D A_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 U_w, S, V_w matrices and the possibly distorted audio signal, the above steps are reversed as follows:

The 1-D audio signal is transformed into a 2-D matrix A_w^*. The * refers to the corruption due to attacks.

The SVD is performed on the possibly distorted watermarked image (A^*_w matrix).

$$A_w^* = U^* S_w^* V^{*T} \tag{5}$$

The matrix that includes the watermark is computed.

$$D^* = U_w S_w^* V_w^T \tag{6}$$

The possibly corrupted encrypted watermark by the channel effects is obtained.

$$W^* = \left(D^* - S\right)/K \tag{7}$$

5. The obtained matrix 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.

IV. Chaotic Encryption

In the proposed algorithm, the embedded image may be encrypted or not. This is according to the level of security required or the importance of this image. Chaotic encryption of the embedded 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 MxM matrix as follows:

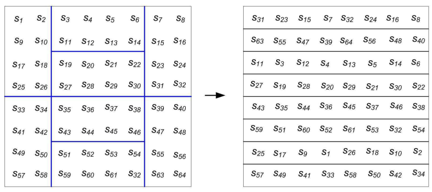
$$B(r,s) = \left[\frac{M}{n_i}(r - M_i) + s \bmod\left(\frac{M}{n_i}\right), \frac{n_i}{M}\left(s - s \bmod\left(\frac{M}{n_i}\right)\right) + M_i\right] \tag{8}$$

where $B(r,s)$ are the new indices of the data item at (r,s), $M_i \le r < M_i + n_i$, $0 < s < M$, and Mi $M_i = n_1 + n_2 + \cdots + n_i$.

In steps, the chaotic encryption is performed as follows:

1- An N × N square matrix is divided into k rectangles of width n_i and number of elements N.
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. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

Figure (1) shows an example of the chaotic encryption of an 8×8 square matrix. The secret key, Skey = (n1, n2, n3) = (2, 4, 2).



Original square matrix. Chaotic encrypted matrix.

Fig 1: Chaotic encryption of an 8 × 8 matrix.

V. The Proposed Algorithm for Bluetooth Networks

Our simulation experiments are carried out over Bluetooth syatem. Due to the limits of the packets size the fragmentation of image is important to complete the transmission. The Bluetooth supports transfer of only small size packets limited form 0-2745 bits that is for classic Bluetooth packets. Our simulation experiments are carried out by using $2DH_1$ packets, $2DH_1$ packet is one of ACL link packets. In this paper, there are two types of packets, standard $2DH_1$ packet and proposed packets through using standard error control codes scheme of old Bluetooth versions, (Hamming (15, 10) code is error control scheme of old versions). Limits of packets lengths lead to fragmentation of bit streams of image. In our simulation, we assume the length of each segment is 512 bits. The process of fragmentation is the last step in our proposed algorithm [17,18].

The fragmentation here is carried out over the watermarked signal A_w (given in equation 4). The 2-D A_w matrix is transformed into a 1-D audio signal. It will be converted to digital data. So, we will get long stream of bits. The size of A_w is 256x256, so the following equation:

$$No\,Segments = \frac{65536 \times 8(\mathrm{Im}ageSize)}{512(ZigbeePacketLength)} \tag{9}$$

$$No\,Segments = \frac{65536 \times 8(\mathrm{Im}ageSize)}{317(ZigbeePacketLength)} \tag{10}$$

Equation 9 gives the number of segments in the case of standard $2DH_1$ packets. The number of segments in the case of encoded $2DH_1$ packets ($2DM_1$) is given by Equation 10. After the fragmentation process is finished, the transmission of packets will start. The choice of the length packets in our simulation has been made to simplify the simulation and fragmentation of the image [19].

At the receiver, the received packets are collected and used to reconstruct the received watermark signal A_w^{*}. After reconstructing the received watermark signal completely, the extracting of embedded image starts. If the embedded image is encrypted, it will be decrypted by chaotic decryption.

VII. Simulation Results

In this section, several experiments are carried out to test the performance of the proposed SVD audio watermarking approach over Bluetooth networks. The Chaotic Baker map is used to encrypt the watermark image as shown in Fig. (2). The encrypted image is then used as a watermark to be embedded in the Handel signal available in Matlab. The Handel waveform is given in Figure (3). In all our experiments, the PSNR is used for the evaluation of the quality of the watermarked audio signals and the correlation coefficient is used to measure the closeness of the decrypted watermark to the original watermark. The following figures show the extracted images and the correlation coefficient values (cr) at different SNR values.

(a) (b)

Fig.(2) Watermark image. (a) Original watermark. (b) Chaotic encrypted watermark cr= 0.0181.

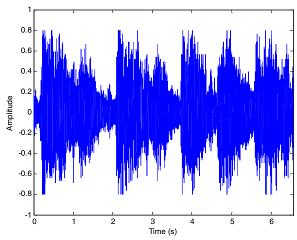
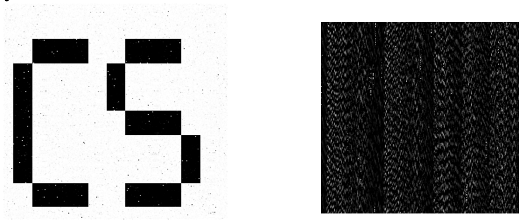


Fig.(3) Original waveform of audio signal

In the first experiment, the proposed SVD audio encrypted watermarking embedding and extraction processes are performed over uncorrelated fading channel through Bluetooth simulation using standard $2DH_1$ packets. The results of experiment are shown in Figs.(4) and (5) at SNR=20 dB and 40 dB, respectively. It is clear from these results that the SVD audio watermarking doesn't degrade the quality of the watermarked audio signal. It is also clear that the watermark is perfectly reconstructed.



(a) (b)

Fig.(4) Watermark image ($2DH_1$). (a) The extracted image at SNR=20dB. (b) The received watermark signal at SNR=20dB, encrypted watermark cr= 0.38.

(a) (b)

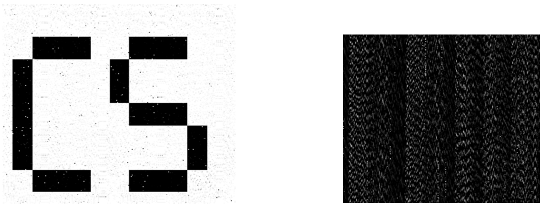
Fig.(5) Watermark image($2DH_1$). (a) The extracted image at SNR=40dB. (b) The received watermark signal at SNR=40dB, encrypted watermark cr= 0.99.

Table 2 gives the results of the previous experiments for different values of SNR. As shown from the extracted images over Bluetooth the SVD audio watermarking doesn't degrade the quality of the watermarked audio signal.

SNR	Correlation Coeff. before Extracting the image	Correlation Coeff. after Extracting the image	PSNR
0 dB	0.318	0.0653	-28.45
10 dB	0.787	0.11	-16.64
20 dB	0.965	0.380	-1.15
30 dB	0.998	0.973	20.04
40 dB	0.9999	0.999	34.61
50 dB	0.9999	0.999	34.61

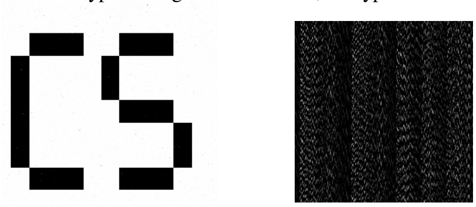
Table 1: the results of SVD-based watermark over Bluetooth systems using standard uncoded packets (over uncorrelated fading channel)

In the second experiment, the previous one is repeated but with using encoded $2DM_1$ packets. The results are shown in Figs. (6) and (7) at SNR 20 dB and 40 dB respectively.



(a) (b)

Fig.(6) Watermark image ($2DM_1$). (a) The extracted image at SNR=20dB. (b) The extracted encrypted image at SNR=20dB, encrypted watermark cr= 0.45.



(a) (b)

Fig.(7) Watermark image($2DM_1$). (a) The extracted image at SNR=40dB. (b) The extracted encrypted image at SNR=40dB, encrypted watermark cr= 0.999.

Table 2 gives the results of the previous experiments for different values of SNR. As shown from the SVD audio watermarking doesn't degrade the quality of the watermarked audio signal.

Also, the experiments reveal using chaotic encryption watermarking with the SVD technique enhances the security over Bluetooth systems and improves the extraction of embedded image, as clear from the results of the provided experiments and the tables of results.

SNR	**Correlation Coeff. before Extracting the image**	**Correlation Coeff. after Extracting the image**	**PSNR**
0 dB	0.332	0.0660	-28.12
10 dB	0.785	0.11	-16.03
20 dB	0.973	0.454	0.926
30 dB	0.9990	0.989	24.71
40 dB	0.9999	0.999	34.711
50 dB	0.9999	0.999	34.711

Table 2: the results of watermark SVD over Bluetooth system using encoded packets (over uncorrelated fading channel)

VIII. CONCLUSIONS

This paper has presented an efficient security algorithm for Bluetooth networks through SVD audio watermarking approach. In this algorithm, an encrypted image is embedded as a watermark in audio signals to achieve a high degree of security. Experimental results have proved that watermark embedding in the proposed approach does not deteriorate the audio signals. It has been clear through experiments that the chaotic Baker map encryption algorithm is an efficient algorithm for watermark encryption. A comparative study between the implementations of the two types of Bluetooth system, encoded and uncoded EDR packets has been provided. Using standard error control codes of Bluetooth schemes gives a little improvement on the extracted watermark image.

References

[1] G. Pekhteryev, Z. Sahinoglu, P. Orlik, and G. Bhatti, "Image Transmission over IEEE 802.15.1 and Bluetooth Networks," IEEE ISCAS May 2005, Kobe Japan.

[2] B. Macq, J. Dittmann, and E. J. Delp, "Benchmarking of Image Watermarking Algorithms for Digital Rights Management", Proceedings 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 Transactions on Image Processing, Vol. 14, No. 6, pp. 822-831, 2005.

[4] H. S. Kim and H. K. Lee, "Invariant Image Watermark Using Zernike Moments", IEEE Transactions on Circuits And Systems For Video Technology, Vol. 13, No. 8, pp. 766-775, 2003.

[5] W. C. Chu, " DCT-Based Image Watermarking Using Subsampling", IEEE Transactions on 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 Transactions on Signal Processing, 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 Transactions on 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 Transactions On Circuits And Systems For Video Technology, 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 Transactions on Signal Processing, Vol. 51, No. 4, pp. 1088-1097, 2003.

[10] G. M. Waleed, M. Faizal, R. B. Ahmed, M. Fareq, B. Abd Malek, and M. Alif Ghani "Bluetooth Wireless Network Authentication Using Radio Frequency Communication protocol", Journal of Computer Science 5 (9): 646-650,2009.

[11] "IEEE 802.15.1 Wpan-Ir Task Group," http:// ww.ieee802.org/15/pub/TG4.html.

[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 802.15.1", IJCSNS International Journal of Computer Science and Network 20 Security, VOL.7 No.7, July 2007

[13] B. P. Lathi , Modern digital and analog communication systems, 2nd edition , Holt, Rinehart and Winston,

[14] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactions On 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", Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

[16] X. Zhu, J. Zhao and H. Xu, "A Digital Watermarking Algorithm and Implementation Based on Improved SVD", Proceedings of The 18th International Conference on Pattern Recognition (ICPR'06).

[17] X. Zhu, J. Zhao and H. Xu, "A Digital Watermarking Algorithm and Implementation Based on Improved SVD", Proceedings of The IEEE 18th International Conference on Pattern Recognition (ICPR'06).

[18] P. Kinney, "Bluetooth Technology: Wireless Control that Simply Works", Communication Design Conference, 2 Oct. 2003.

[19] B. Kai, and P. Yong, "Performance Study on Bluetooth-Based Wireless Personal Area Networks for Real-Time Health monitoring", ETRI Journal, Volume 28, No. 4, Aug. 2006.