Multimedia Filter for Data Hiding Counteraction

Zbigniew Piotrowski
Faculty of Electronics, Military University of Technology
Gen. S. Kaliskiego 2 str., Warsaw 00-908, Poland

Abstract— Data hiding methods are realised in the form of steganographic communication channels and in the form of digital content labelled with watermark while employing as the carrying layer among the others: speech signal, audio, video and photos. Detection of the fact of additional data hiding is hindered among the others because of constantly improved and increasingly advanced methods for embedding and extraction of hidden data. In the article there is presented the concept of the program container based on which the filtration of the above-mentioned signals is carried out in order to remove the hidden data. The purpose of multimedia filter action is to remove from the original signal (carrier) the hidden data or its significant degradation, but in such manner that the original signal itself is not degraded significantly.

1. INTRODUCTION

The methods of the hidden data removal from the multimedia content are well known. In [1] three types of attacks are described taking into account the available knowledge about the watermark structure, embedder and extractor. These attacks include: exploiting the design weakness via blind attack (I), exploring the knowledge based on embedding and extracting processes using original signal and watermarked one (II) and the last type is a combination of the two (III). The first type attack does not depend on the knowledge about the watermark embedding method. Such attacks include the basic methods for signal processing, e.g., resampling, analogue-to-digital and digital-to-analogue conversion, noise addition, lossy compression [2]. The second type attack is possible thanks to the signal analysis before and after embedding the hidden data. The signal analysis is conducted in both time and frequency fields, and considering among the others: system frequency response. The discovered differences may be the essential prerequisite for recognising the method of watermark embedding or the structure of the steganographic sequence. The attacks on the hidden data may be hindered in a defence manner described in [3] in the form of hidden data masking. The authors of the articles suggested the technique named *Data Masking* which consists in forming the Probability Density Function (PDF) of the information enciphered to PDF format similar to the audio or video signal stream. This way, the probability distribution of the enciphered data occurrence becomes similar to the statistic distribution represented by audio or video signals. As it was stated in [3] the attacks conducted by traditional stego-analysers of the hidden information on so-masked confidential data are of low effectiveness.

As it was specified in the publication [4] among the attacks on the hidden data contained in the multimedia signal there can be distinguished: removal attacks, geometric attacks, cryptographic attacks, estimation-based attacks, remodulation attacks, copy attack, synchronisation removal. The filter for removing the hidden data in the multimedia content may both remove the hidden data from the multimedia content and degrade the hidden data (represented by the watermark signal or steganographic sequence) in such way that they become impossible for extraction at the receiving side, simultaneously meeting the condition of keeping the original signal quality at the acceptable level by the user. The article proposes to apply the multimedia filter whose task is to remove the potentially occurring hidden data contained in the audio streams, video streams or in the multimedia files. It is assumed that the filter may operate also on the speech signal in the telephony systems [5]. The methods for embedding the hidden data in the video and audio signals are known [6–10]. The filter having the transmittance $H(z)$ matched depending on the selected method taken from the block of the method container DSP, makes the filtration of the signal which can potentially have the embedded hidden data. To the filter it is possible connect the digital routes from the telephone exchange PSTN/VoIP or Internet server whose task would be the filtration of the data streams or selected Internet resources. By means of testing the signal quality and fidelity before and after the filtration, it is possible to choose such processing parameters of the filter that the processed signal degradation can be minimised [11–13].

In case of the hardware realisation of the proposed multimedia filter, you should pay attention to the question of the equipment electromagnetic shielding and its electromagnetic compatibility [14–22]. The essential part of the network environment for the described multimedia filter is the

possibility of operation in the heterogenic environment with the guarantee for providing the service quality [23–25].

As the degraded signal metrics there may be used the following norms:

Maximum Difference:

$$MD = \max \left| A_n - A'_n \right|$$

Average Absolute Difference:

$$AD = \frac{1}{N} \sum_n \left| A_n - A'_n \right|$$

Normalized Average Absolute Difference:

$$NAD = \frac{\sum_n |A_n - A'_n|}{\sum_n |A_n|}$$

Mean Square Error:

$$MSE = \frac{1}{N} \sum_n \left(A_n - A'_n \right)^2$$

LP-Norm:

$$LP = \left(\frac{1}{N} \sum_n \left| A_n - A'_n \right| \right)^{1/p}$$

Signal to Noise Ratio:

$$SNR = \frac{\sum_n A_n^2}{\sum_n \left(A_n - A'_n \right)^2}$$

Audio Fidelity (AF):

$$AF = 1 - \frac{\sum_n \left(A_n - A'_n \right)^2}{\sum_n A_n^2}$$

where: A_n — original signal, A'_n — filtered signal, n — number of sample.

2. MULTIMEDIALNY FILTR SKRYTYCH DANYCH

The described concept of the multimedia filter is presented in the Figure 1.

The filter for removing the hidden data contains in its structure (Figure 1) the executive module in the block form: multimedia filter, with the transmittance $H(z)$ shaped by the method container DSP and parameters of DSP methods named DSP container. The degradation degree of the filtered signal is verified depending on the input content and the selected method of filtration in the block multimedia content quality testing and filter parameters adaptation.

In the Figure 2 there is presented an example positioning of the multimedia filter for removing the hidden data. It may work in the cascade mode, just after the module for the dedicated attack methods on the hidden data, or in the parallel mode. The filter may be installed, e.g., in the routers

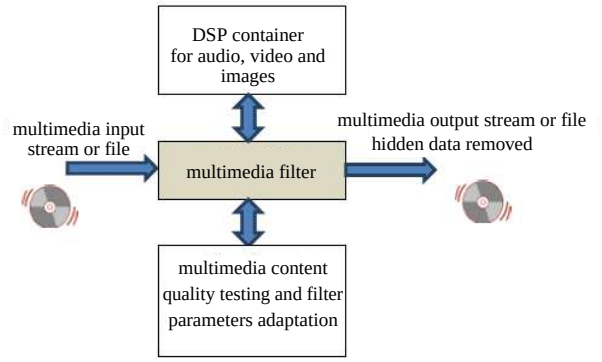

Figure 1: Multimedia filter for hidden data removal.

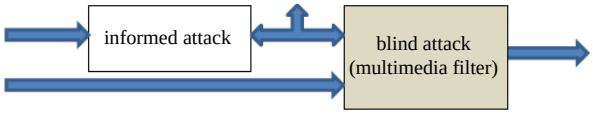

Figure 2: Configuration of the attack methods on the hidden data.

(while using the network technique *Deep Packet Inspection*, DPI — in order to scan the datagrams containing the multimedia signal), in the telephone exchanges or in the commonly used equipment, e.g., smartphones, PSTN telephones etc., protecting against hidden steganographic transmission and against penetration of the devices and telecommunication infrastructure at the same time. The filter may also be the part of automatic scanner for computer viruses scanning the particular resources of the computer.

3. CONCLUSIONS

In the article there is presented the concept of the multimedia filter for removing the hidden data. The filter has its application in the filtration of the digital multimedia signal in order to remove or degrade significantly the hidden data represented by the watermark or steganographic sequence sent, e.g., in the speech signal in the telephonic connections.

The filter can carry out such operations on the signal as: lossy compression, re-quantization, resampling, all-pass the filtration, equalisation, noise addition etc.. The filter, depending whether the following are known: watermark structure, steganographic sequence, embedding method or extraction method for the hidden data, may work on any input signal while using the selected set of methods so-called blind attack or informed attack. The multimedia filter may be the complementation of the hidden transmission stego-analyser. In the presented concept of the system, it is necessary to model the individual parameters of the filtration depending on the quality of the digital content and assumed degree of the signal degeneration.

REFERENCES

1. Wu, M. and B. Liu, *Multimedia Data Hiding*, Springer-Verlag, 2002, ISBN: 0-387-95426-0.
2. Test Result of International Evaluation Project for Digital Watermark Technology for Music, 2000, http://www.nri.co.jp/english/news/2000/001006.html.
3. Radhakrishan, R., M. Kharrazi, and N. Memon, "Data masking: A new approach for steganography?," *Journal of VLSI Signal Processing*, Vol. 41, 293–303, 2005.
4. Voloshynovskiy, S. and T. P. Pereira, "Attacks on digital watermarks: Classification, estimation-based attacks and benchmarks," *IEEE Communications Magazine*, Vol. 39, No. 8, 118–126, 2002, ISSN: 0163-6804.
5. Piotrowski, Z. and W. Grabiec, "Voice trust in public switched telephone networks," *MCSS 2012, Communications in Computer and Information Science, CCIS 287*, 282–291, Springer, Heidelberg, 2012, ISBN: 978-3-642-30720-1.
6. Lenarczyk, P. and Z. Piotrowski, "Parallel blind digital image watermarking in spatial and frequency domains, telecommunication systems," *Telecommunication Systems*, Vol. 54, 287–303, 2013, Doi: 10.1007/s11235-013-9734-x.
7. Piotrowski, Z., "Drift correction modulation scheme for digital signal processing," *Mathematical and Computer Modelling*, Vol. 57, Nos. 11–12, 2660–2670, Elsevier, Jun. 2013, Doi: 10.1016/j.mcm. 2011.09.016.
8. Piotrowski, Z., "The national network-centric system and its components in the age of information warfare," *Safety and Security Engineering III, SAFE III*, 301–309, WIT Press, Southampton, Boston, 2009, ISBN: 978-1-84564-193-1, ISSN: 1746-4498, ISSN: 1743-3509.
9. Piotrowski, Z., "Angle phase drift correction method effectiveness," *Signal Processing Algorithms, Architectures, Arrangements, and Applications Conference Proceedings (SPA)*, 82–86, Poznan, 2009, ISBN: 978-83-62065-00-4.
10. Piotrowski, Z. and P. Gajewski, "Novel method for watermarking system operating on the HF and VHF radio links," *Computational Methods and Experimental Measurements XIII, CMEM XIII*, 791–800, WIT Press, Southampton, Boston, 2007, ISBN: 978-1-84564-084-2, ISSN: 1746-4064, ISSN: 1743-355X.
11. Piotrowski, Z. and P. Gajewski, "Fidelity estimation of watermarked audio signals according to the ITU-R BS.1116-1 standard," *Acta Physica Polonica A, Acoustic and Biomedical Engineering*, Vol. 121, No. 1-A, 82–85, 2012, ISSN: 0587-4246.
12. Piotrowski, Z., "Precise psychoacoustic correction method based on calculation of JND level," *Acta Physica Polonica A, Optical and Acoustical Methods in Science and Technology*, Vol. 116, No. 3, 375–379, 2009.
13. Piotrowski, Z. and P. Gajewski, "Acoustic watermark server effectiveness," *Computational Methods and Experimental Measurements XIV, CMEM XIV*, 251–258, WIT Press, Southampton, Boston, 2009, ISBN: 978-1-84564-187-0, ISSN: 1746-4046, ISSN: 1743-355X.

14. Nowosielski, L., M. Wnuk, and C. Ziółowski, "Interlaboratory tests in scope of measurement of radio disturbance," *European Microwave Week 2009, EuMW 2009: Science, Progress and Quality at Radiofrequencies, Conference Proceedings — 39th European Microwave Conference, EuMC 2009*, Article No. 5296286, 288–291, 2009.
15. Nowosielski, L., J. patka, and M. Siłczuk, "Modelling of electromagnetic wave propagation with the use of the ray-tracing method," *PIERS Proceedings*, 2701–2705, Guangzhou, China, Aug. 25–28, 2014.
16. Nowosielski, L. and C. Piotrowski, "Honeycomb ventilation grill shielding effectiveness measuring methodology," *PIERS Proceedings*, 2692–2696, Guangzhou, China, Aug. 25–28, 2014.
17. Nowosielski, L. and M. Wnuk, "Compromising emanations from USB 2 interface," *PIERS Proceedings*, 2666–2670, Guangzhou, China, Aug. 25–28, 2014.
18. Kaszuba, A., R. Checinski, M. Kryk, J. Lopatka, and L. Nowosielski, "Electromagnetically shielded real-time MANET testbed," *PIERS Proceedings*, 2706–2710, Guangzhou, China, Aug. 25–28, 2014.
19. Nowosielski, L. and J. Lopatka, "Measurement of shielding effectiveness with the method using high power electromagnetic pulse generator," *PIERS Proceedings*, 2687–2691, Guangzhou, China, Aug. 25–28, 2014.
20. Gruszczynski, M., M. Wnuk, and L. Nowosielski, "Multisystem microstrip antenna for mobile communications," *IEEE Antennas and Propagation Society, AP-S International Symposium (Digest)*, Article No. 6349179, 2012.
21. Nowosielski, L., M. Wnuk, and C. Ziółkowski, "Interlaboratory tests in scope of measurement of radio disturbance," *European Microwave Week 2009, EuMW 2009: Science, Progress and Quality at Radiofrequencies, Conference Proceedings — 39th European Microwave Conference, EuMC 2009*, Article No. 5296286, 288–291, 2009.
22. Piotrowski, Z., L. Nowosielski, L. Zagoździński, and P. Gajewski, "Electromagnetic compatibility of the military handset with hidden authorization function based on MIL-STD-461D results," *PIERS Online*, 566–570, 2008.
23. Lubkowski, P., M. Bednarczyk, K. Maslanka, and M. Amanowicz, "QoS-aware end-to-end connectivity provision in a heterogeneous military environment," *Military Communications and Information Systems Conference 2013*, Saint Malo, France, 2013.
24. Lubkowski, P. and D. Laskowski, "Provision of the reliable video surveillance services in heterogeneous networks," *European Safety and Reliability Conference, ESREL 2014*, Wroclaw, Poland, Accepted for Publication, 2014.
25. Hauge, M., L. Landmark, P. Lubkowski, M. Amanowicz, and K. Maslanka, "Selected issues of QoS provision in heterogenous military networks," *International Journal of Electronics and Telecommunications*, Vol. 60, No. 1, 7–13, 2014.