Optimization of Demodulation for Air–Gap Data Transmission based on Backlight Modulation of Screen

Dawid Bak[1][0000−0003−0774−9738],
Przemyslaw Mazurek[2][0000−0001−6403−4160], and
Dorota Oszutowska–Mazurek[3][0000−0002−7145−3993]

[1] Department of Signal Processing and Multimedia Engineering,
West Pomeranian University of Technology Szczecin, Szczecin, Poland
dawid.bak@zut.edu.pl
[2] przemyslaw.mazurek@zut.edu.pl
[3] Department of Epidemiology and Management,
Pomeranian Medical University, Szczecin, Poland
adorotta@pum.edu.pl

Abstract. Air–gap is an efficient technique for the improving of computer security. Proposed technique uses backlight modulation of monitor screen for data transmission from infected computer. The optimization algorithm for the segmentation of video stream is proposed for the improving of data transmission robustness. This algorithm is tested using Monte Carlo approach with full frame analysis for different values of standard deviations of additive Gaussian noise. Achieved results show improvements for proposed selective image processing for low values of standard deviation about ten times.

Keywords: Air–Gap Transmission · Digital Demodulation · Image Processing · Network Security · Monte Carlo Simulations

1 Introduction

Problems of computer security is currently one of the most important problems of technical civilization. There are many methods of attacking computers or computer networks, in particular remote methods that do not require direct access.

The emergence of this type of problem resulted in the emergence of a number of defense methods. Some of these methods use technical means, such as firewalls or antivirus programs. Users' awareness of possible threats is also important for the security of computers or computer networks. Organizational security methods are, for example, software or hardware audits.

Air–gap is a very efficient method of improving the security of individual computers or computer systems [6]. Isolation through the lack of communication interfaces reduces the possibility of attacks. Air–gap breaking by the establishing

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

unconventional communication interfaces is possible by the infection of secured computer or computer system [7]. The methods used for infection are not taken into account in this work.

Establishing one–way or two–way communication is important for both attackers and for prevention that is important for security engineers [8]. The data rate achieved is usually very low: a single bit is sent per second. Such transmission allows attack on PIN codes, passwords and very short confidential data. A typical air–gap attack is a one-way attack where data is sent outside of a protected computer or computer network. This type of attack is a long–term process that requires the attacker to listen in close proximity to the protected area.

1.1 Content and Contribution of the Paper

Air–gap transmission techniques are very active research area and some recent development are related to the application of different physical mediums. Example optical channels are: QR code embedding in image [13] (VisiSploit), network LEDs modulation in routers [18] (xLED), infrared transmission [16] (aIR–Jumper). Radio based transmission attacks are for example: USBee [15], AirHopper [14] and GSMem [17]. These types of transmission channels are not covered by typical protection, in particular audits, and therefore are very dangerous. Intentional data transmission hiding could be used for monitoring devices also [21].

In previous works, we proposed using a computer screen flashing for data transmission [4, 5]. In the absence or very low user activity, very small changes in screen brightness are used that are not noticeable to humans.

It is possible to receive data correctly from a large distance using image observation with a camera and a telescope, as well as digital image processing and demodulation algorithms A typical modulation applied in this type of solutions is BFSK (Binary Frequency–Shift Keying) [10, 19], which allows estimation of transmission settings like symbol and keyed frequencies [5].

Previous work assumed the processing of full–frame video sequences for estimation the transmitted signal [5]. Each frame of the image was transformed by averaging to a single value, i.e. the video sequence was converted into a one-dimensional signal The signal analysis for a single image pixel is not effective due to the low SNR (Signal–to–Noise Ratio) value. Averaging the whole frame of the image allows improved SNR, and the best solution is to average only the selected image area, such as the computer screen image. The problem dealt with in this article is the automatic determination of the area subjected to averaging. Determining the image area where brightness modulation occurs allows the SNR to be improved, because areas where there is no modulation are just a source of undesirable noise. This is particularly important in the case of an indirect attack, where the computer screen is not visible directly, but only the glow in the room is visible (Fig. 1). Very often screens of computers and keyboards, for security reasons, are set so that they are not visible from the outside.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

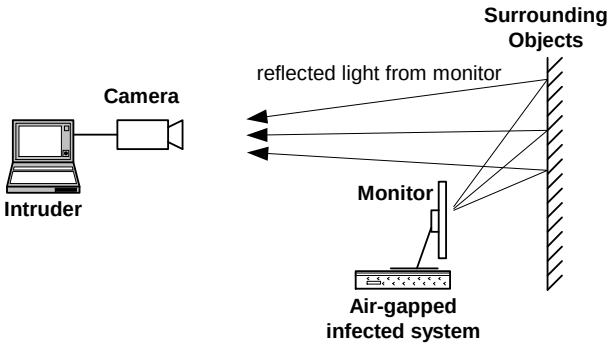

Fig. 1. Scheme of measurement of monitor brightness changes.

What's more, diffusion foils are used to block the possibility of direct observation of the room through the windows, but diffusion foils does not eliminate the glow of monitors.

The application of the optimization algorithm allows searching in the frame for the image of areas for which the brightness changes are the greatest to reduce the impact of noise. Areas for which the brightness changes are small bring the most noise to the signal and should be omitted in the analysis. Areas that should be omitted are those that are illuminated by other sources (other monitors, sources of light in the room)

The proposed algorithm is an offline algorithm, and the data is processed after recording the video image.

Example scenarios and acquisition configurations are presented in Section 2. Details of algorithm and processing method are considered in Section 3. Result are presented in Section 4 and discussion is provided in Section 5. Final conclusions and further work are considered in Section 6.

2 Data

The evaluation of the algorithm is based on an empirical test as proof of concept

The source of the data is the laptop of which the screen is not visible directly. The laptop has software that modulates the brightness of the monitor. Brightness changes are not visible to a human directly, which means that the signal has a relatively small SNR.

The second laptop is positioned so that its screen is visible in the frame (Fig. 2). This laptop is a source of local interference, due to strong changes in screen brightness. Additional sources of interference are the lamps that illuminate the corridor. The purpose of the optimization algorithm is to detect areas from which transmitted data can be obtained, while avoiding interference areas.

Data is recorded using the ZWO ASI1600MM–COOL camera with a monochromatic sensor [26] and a resolution of 16 Mpix, and Canon EF 100mm 1:2.8L IS

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

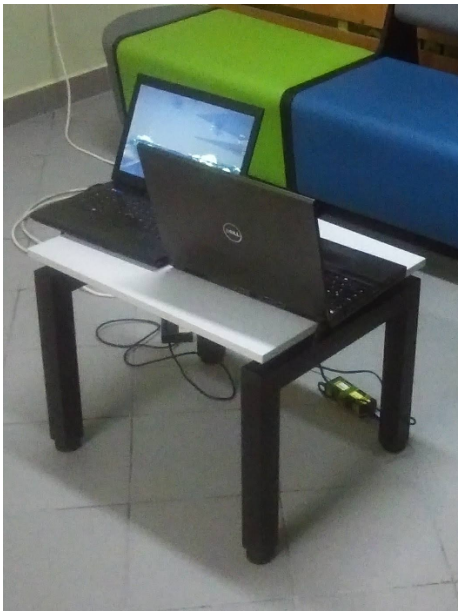

Fig. 2. Light disturbance computer from the left and back of observed computer screen from the right.

USM lenses. The camera was placed on a tripod to ensure video recording without shifting the essential elements of the scene (Fig. 3).

ASICAP v.1.3 software for MS Windows and USB 3.0 interface has been used for video sequence acquisition. The camera sensor supports ROI (Region of Interest), that is used to reduce USB bandwidth and storage requirements, so the recorded picture frames have a resolution of 1024×768. Measured HFOV (Horizontal Field of View) is about 3° for the selected ROI, and the distance between the camera and the computer screen is about 29 meters. This camera has advanced cooling (thermoelectric cooler and fan) for sensor noise reduction, but this option was not used. Recording speed is 100fps and 10ms exposure time is selected for the flickering reduction due to fluorescent lamps sources in corridor. Recorded video sequences are of high quality because they are raw frames, which enables to control the influence of noise (Fig. 4).

3 Method

Direct observation of the computer screen is sometimes not possible due to spatial relations. The light emitted by the computer screen can be observed indirectly by reflections from the surrounding objects. Glass, plastic, metal materials are particularly interesting because they can reflect light strongly in a specific direction. The Lambertian surfaces are also interesting because the light is scattered in all directions.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

Fig. 3. Acquisition system.

Fig. 4. Light disturbance computer from the left and back of observed computer screen from the right (camera view).

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

An optimization algorithm, based on local full–frame search, is required to process as many picture frames as possible using the demodulation algorithm. Signal processing part is described in [4] and [5]. The detection using two band–pass filters and rectifiers was proposed in [19] and is not considered in this paper. There are two sources of interfering signals: light sources and camera noise. The input image is reduced to 16×12 pixels for reducing picture noise and processing complexity.

The aim of proposed algorithm is the calculation of segmented image S with positive pixel values $S(x, y)$ that corresponds to segmented area number. Pixel position (x, y) corresponds to the signal from video sequence $V(x, y, k)$, where x and y are image coordinates and k is the frame number. Two pixels S_i and S_j belong to the same segmented area $S_i(.,.) = s$ and $S_j(.,.) = s$ if the similarity between corresponding video sequences is found using Euclidean metric:

$$d(i,j) = \left(\sum_k \left(V_i(x_i, y_i, k) - V_j(x_j, y_j, k) \right)^2 \right) < T, \tag{1}$$

where T is threshold and $d(i, j)$ binary value (1 - similar, 0 - not similar).

The problem is the number of calculations required for $d(i, j)$, large image resolutions and long sequences. Local comparisons can be used to reduce the calculation due to spatial similarity and this variant is considered.

Algorithm randomly selects starting position (x_i, y_i) uses spatial neighborhoods:

$$(x_i - 1, y_i), \tag{2}$$
$$(x_i + 1, y_i), \tag{3}$$
$$(x_i, y_i - 1), \tag{4}$$
$$(x_i, y_i + 1) \tag{5}$$

as a second position (x_j, y_j) if they are not assigned to any s. New positions are marked as possible points for starting new comparisons with own neighborhoods. This algorithm behaves like local fill algorithm [25]. This process is repeated until the assignment to the same s region is possible. New position is randomly selected from not assigned yet positions to any s with new s value and repeated until all positions are not used.

Modified distance criteria (1) should be used due to the problem of direct comparison of values. Adjacent pixels can be illuminated in the same way, but with different average values, so the basic algorithm (1) discards pixels that, for example, belong to different scene objects, even if the lighting changes are similar. Proposed algorithm uses the removal of mean values using the following formulas:

$$d^*(i,j) = \left(\sum_k \left(V_i^*(x_i, y_i, k) - V_j^*(x_j, y_j, k) \right)^2 \right) < T, \tag{6}$$

$$V^*(x, y, k) = V(x, y, k) - mean\left(V(x, y, .)\right), \tag{7}$$

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

where V^* is corrected V sequence and $d^*(i,j)$ is a new similarity metric.

The threshold value is adaptively selected by testing the number of areas achieved, and the number of areas should typically be $5-20$, so multiple passes of the segmentation algorithm are necessary to select the threshold value. Demodulation is processed individually for each A_s area with a common value of s. This area uses the following signal fusion formula:

$$A_s(k) = \frac{1}{N_s} \sum_s \left(V(x,y,k) - mean\left(V(x,y,.) \right) \right), \tag{8}$$

where N_s is the number of pixels with the same $S(x,y) = s$ assignment.

Each demodulated sequence should be checked using an additional CRC (Cyclic Redundancy Check) code for the final selection of the sequence of bits and this topic is out of the scope of the paper.

4 Results

Basic method of air gap transmission using the computer screen brightness changes assumes BFSK modulation and 0.18 bit/s transmission is used. The speed results from assumed slow changes in the brightness of the monitor screen. The Hamming distance between known and received binary sequences is used as the quality criterion. Binary keying signals that have higher resolution are used instead of comparison of demodulated bits. This approach reduces final result influences in demodulation algorithm.

Additive Gaussian noise images with known and controlled standard deviation are applied to all video frames in order to analysis of the sensitivity. Particular video sequence is tested 100 times for the selected standard deviation value and number of segmented region in $5-20$ range.

Box and whisker plots for full frame processing and selective processing are shown in Fig. 5. These Monte Carlo test [22] allows the comparison of algorithm and the determination of properties basing on intensive numerical tests. Example segmentation results are shown in Fig. 6.

5 Discussion

Obtained results (Fig. 5) show importance of proposed solution. Achieved segmentation results influences Hamming errors. Proposed solution gives about ten times less errors comparing to entire image frame processing. Noised video sequences introduces Hamming errors, but proposed algorithm is still superior (Fig. 5). The results presented using the Monte Carlo analysis show how the signal degradation curve behaves for many tests for different standard deviation values of the interfering video noise.

The computing cost is very large for the proposed algorithm, because the entire video sequence is analyzed. It is possible to reduce it by the application only to a short sequence. Obtained area of interest can be used for the selection

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

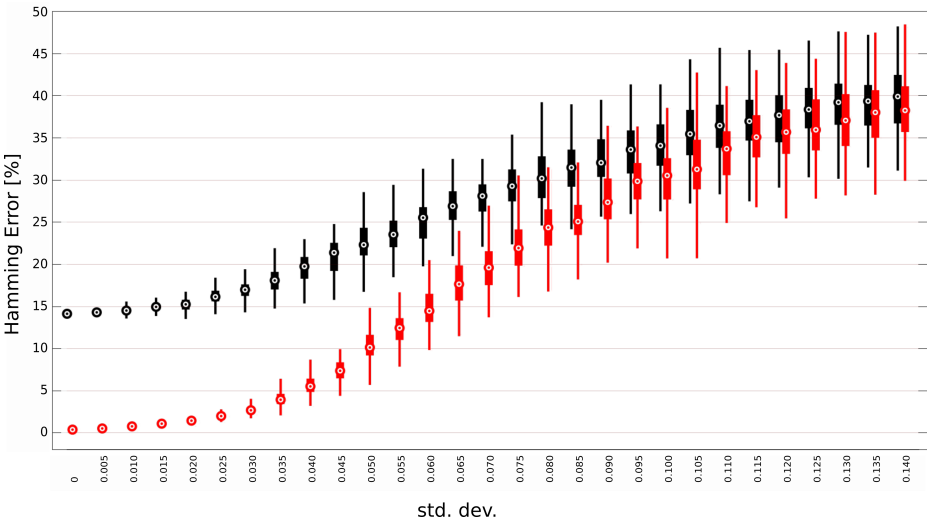

Fig. 5. Monte Carlo analysis of Hamming errors for full frame (black) and selective processing (red) algorithms.

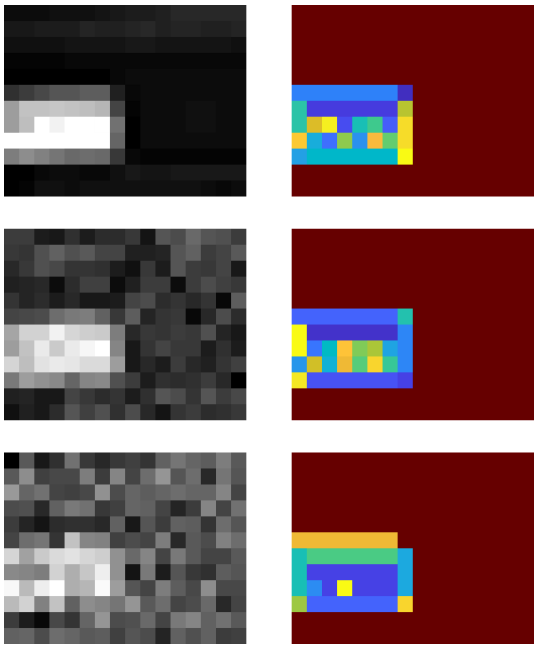

Fig. 6. Examples of processed image (top) and segmented regions (bottom) after rescalling with additive Gaussian noise with std.dev.: 0 (top), 0.055 (middle) and 0.120 (bottom).

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

of a pixel for the entire video sequence. The largest regions in Fig. 6 are exemplary results of the proposed algorithm (marked using dark red color). This area includes both the background behind the monitor and the monitor housing, so it is not an optimal area, which requires the selection of a different threshold value. The obtained results, however, show how strong the level of interference from the monitor with the directly visible screen (Fig. 5).

The backlight modulation can be used for transmission of data from a room with diffusers in the windows The diffusers are used for protection against direct observation of the computer screen using a telescope. This method also accepts blurred images.

The cost of the calculations depends on the image resolution, so quite small resolution has been used. A serious problem is the necessity of processing quite long video sequences (Equations (7) and (8)). Processing using OpenMP [9], MPI [20, 24] and CUDA [12, 23] is possible for the considered algorithm.

6 Conclusions and Further Work

Backlight modulation of computer screen is very import technique for air–gap data transmission and proposed segmentation extends possibilities by the automatic selection of video region. Light reflection from walls and surrounding objects could be used, if no direct visibility of screen is possible.

Optical techniques for the data transmission requires direct visibility of source, but this method shows the possibility of indirect data transmission. Very important property of the optical techniques is the possible large distance observation using telescopes and high sensitivity cameras.

The search task for the best area having the largest SNR can be performed using the optimization algorithm [1–3, 11]. In addition, the selection of the threshold T value can also be performed automatically using the optimization algorithm. These tasks will be the subject of further work.

Additional further work will be related to the improving of bit rate also, because it is important limitation for numerous air–gap communication methods. Such improvement gives better utilization of short time slots without user activities that could disturb data transmission.

Acknowledgment

This work is supported by the UE EFRR ZPORR project Z/2.32/I/1.3.1/267/05 "Szczecin University of Technology – Research and Education Center of Modern Multimedia Technologies" (Poland).

References

1. Abualigah, L.: Feature Selection and Enhanced Krill Herd Algorithm for Text Document Clustering. Studies in Computational Intelligence, Springer (12 2018)

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

2. Abualigah, L., Khader, A.T., Said Hanandeh, E.: A combination of objective functions and hybrid krill herd algorithm for text document clustering analysis. Engineering Applications of Artificial Intelligence **73** (May 2018)
3. Abualigah, L.M., Khader, A.T.: Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering. The Journal of Supercomputing **73**(11), 4773–4795 (Nov 2017)
4. Bak, D., Mazurek, P.: Air–gap data transmission using screen brightness modulation. In: 2018 International Interdisciplinary PhD Workshop (IIPhDW). pp. 147–150 (May 2018)
5. Bak, D., Mazurek, P.: Air–gap data transmission using backlight modulation of screen. In: Choraś, M., Choraś, R.S. (eds.) Image Processing and Communications Challenges 10. pp. 96–103. Springer International Publishing (2019)
6. Bryant, W.: International conflict and cyberspace superiority: Theory and practice. International Conflict and Cyberspace Superiority: Theory and Practice pp. 1–239 (01 2015)
7. Carrara, B.: Air-Gap Covert Channels. Ph.D. thesis, School of Electrical Engineering and Computer Science, Faculty of Engineering, University of Ottawa (2016)
8. Carrara, B., Adams, C.: Out-of-band covert channels—a survey. ACM Comput. Surv. **49**(2), 23:1–23:36 (Jun 2016)
9. Chapman, B., Jost, G., Pas, R.v.d.: Using OpenMP: Portable Shared Memory Parallel Programming (Scientific and Engineering Computation). The MIT Press (2007)
10. Chitode, J.: Digital Communication. Technical Publications (2010)
11. Engelbrecht, A.P.: Fundamentals of Computational Swarm Intelligence. John Wiley and Sons, Inc., USA (2006)
12. Farber, R.: CUDA Application Design and Development. Morgan Kaufmann (2011)
13. Guri, M., Hasson, O., Kedma, G., Elovici, Y.: An optical covert-channel to leak data through an air-gap. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). pp. 642–649 (Dec 2016)
14. Guri, M., Kedma, G., Kachlon, A., Elovici, Y.: Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In: 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). pp. 58–67 (Oct 2014)
15. Guri, M., Monitz, M., Elovici, Y.: Usbee: Air-gap covert-channel via electromagnetic emission from usb. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). pp. 264–268 (Dec 2016)
16. Guri, M., Bykhovsky, D., Elovici, Y.: air–jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR). CoRR **abs/1709.05742** (2017)
17. Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., Elovici, Y.: Gsmem: Data exfiltration from air-gapped computers over GSM frequencies. In: 24th USENIX Security Symposium (USENIX Security 15). pp. 849–864. USENIX Association, Washington, D.C. (2015)
18. Guri, M., Zadov, B., Daidakulov, A., Elovici, Y.: xled: Covert data exfiltration from air-gapped networks via router leds. CoRR **abs/1706.01140** (2017)
19. Haykin, S.S.: Digital Communications. Wiley-India (1988)
20. Karniadakis, G., Kirby, R.: Parallel Scientific Computing in C++ and MPI. Cambridge University Press (2003)

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6

21. Mazurek, P., Bak, D.: Embedded Software Monitoring Using Pulse Width Modulation as a Communication Channel for Low Pin Count Microcontroller Applications, pp. 319–330 (01 2019)
22. Metropolis, N.: The Beginning of the Monte Carlo Method. Los Alamos Science (1987), http://library.lanl.gov/la-pubs/00326866.pdf
23. Sanders, J., Kandrot, E.: CUDA by Example: An Introduction to General–Purpose GPU Programming. Addison–Wesley (2010)
24. Snir, M., Otto, S., Huss-Lederman, S., Walker, D., Dongarra, J.: MPI: The Complete Reference. MIT Press (1996)
25. Torbert, S.: Applied Computer Science. Springer, 2nd edn. (2016)
26. ZWO: ASI1600 Manual (2016), revision 1.1

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22734-0_6