Towards Preventative Steganalysis in Wireless Visual Sensor Networks

Julien S. Jainsky [1], Deepa Kundur [2]

Electrical and Computer Engineering Department, Texas A&M University

[1] julienj@tamu.edu; [2] dkundur@tamu.edu

***Abstract*- Issues of security and privacy in surveillance systems are abound. Much focus has been put toward developing security strategies for emerging wireless visual sensor networks. Solutions target protection of the overt communication channel. However, given the characteristics of these networks which include shared resources, high degrees of collaboration and the presence of redundancy and uncertainty, they represent a rich environment for the presence of covert communications. Thus, we assert that threat models for such systems must include steganographic models. In this paper, we present the problem of preventative steganalysis that addresses steganographic issues in wireless visual sensor networks. The goal of preventative steganalysis is to offer a proactive solution against steganography by increasing the steganalyst's knowledge of the cover-media and thus emphasizing the presence of hidden messages. This paper introduces the topic of preventative steganalysis. Characteristics of an effective steganographic solution are derived and a practical solution is tested.**

Keywords*- *Steganography; Steganalysis; Wireless Visual Sensor Network

I. INTRODUCTION

It is well known that wireless visual sensor networks (WVSNs) can be used in a wide range of applications from the surveillance of potentially dangerous areas, such as war zones, to habitat monitoring including the supervision of animal territories. Because of their relatively low cost, small component size and reasonable autonomy, WVSNs enable environmental monitoring in areas considered to be hostile for direct human interaction. Given their image capturing capabilities, WVSNscan record huge volumes of data which, depending on the application, can carry private and sensitive information. For this reason security and privacy is of fundamental concern for WVSN development and use.

Much research activity has been dedicated to the investigation of security issues in the overt communication infrastructure of a WVSN. In this paper, we investigate WVSN security in the context of covert communications. Specifically, we introduce and present the problem of preventative steganalysis. We highlight the steganographic security concerns in visual sensor networks and describe the competing goals of the steganographer (a party involved in covert communications) and the steganalyst (a party attempting to discourage covert activity through network development and operation) in order to derive system design principles to either mitigate or limit steganalytic activity in WVSNs. Asteganalytic solution is developed and applied to a real case of WVSN video surveillance to illustrate the functionality of our approach.

II. BACKGROUND

Most well-known measures to protect WVSNs, to date, have focused on the problem of providing privacy in vision-rich systems. Lo *et al.* [1] introduced an automated homecare monitoring system for the elderly named *UbiSense* where image processing is conducted directly at the camera to convert visual data directly into abstractions that reveal no personal information and hence protect the privacy of the monitored individuals. Fidaleo *et al.* [2] introduced the *Networked Sensor Tapestry (NeST)* architecture designed for the secure sharing, capture, and distributed processing and archiving of multimedia data. They introduce the notion of "subjective privacy" in which processing of raw sensor data is conducted to remove personally identifiable information; thus the behavior, but not the identity of an individual under surveillance is conveyed. The resulting data, approved for public viewing, are communicated in a network that employs the secure socket layer protocol and client authorization for network-level protection. Wickramasuriya *et al.* [3] presented a privacy preserving video surveillance system that monitors subjects in an observation region using video cameras along with motion sensors and RFID tags. The motion detectors are used to trigger the video cameras on or off, and the RFIDs of the subjects provide authorization information in order to specify which individuals are entitled to privacy and hence have their visual information masked through image processing. Kundur *et al.*[4] presented the HoLiSTiC (Heterogeneous Lightweight Sensornet for Trusted Visual Computing) framework for WVSN security that exploits secure protocols in a hierarchical directional link communication network to achieve broadband low power communications. A decentralized visual secret sharing approach is used to preserve privacy.

More recently, research has also emerged with the goal of assuring the authenticity of the data collected by sensor networks. When nodes are corrupted and provide false information, the entire network's legitimacy is compromised. The authentication of each node allows for the network to remain trusted. Several proposed solutions utilize common cryptographic concepts to provide such security. Feng *et al.* [5] introduced a paradigm to cryptologically embed signatures into the collected data via watermarking techniques. Their objective is to efficiently watermark the data while introducing as little distortion as possible. Zheng *et al.* [6] proposed to offer authenticity assurance using a public key cryptographic scheme. A derivable public key scheme is used which has the effect of simplifying the cryptography and reducing the need for key storage,

therefore making it more suitable for large scale sensor networks. Because these methods still increase the workload of the WSN, Martinovic *et al.* [7] proposed a novel paradigm that relies on the properties of wireless communications to provide authentication capabilities. They focus their study on taking advantage of frequency jamming to detect attacks and strengthen the WSN's security. Given the need for energy conservation in distributed wireless networks, Blaß *et al.* [8] developed Extended Secure Aggregation for Wireless Sensor Networks (ESAWN). ESAWN finds a trade-off between decreasing the energy consumption of the network via data aggregation and providing authentication mechanisms that are fundamentally weaker compared to techniques that are not driven by energy preservation.

These existing approaches for WVSN protection all focus on protecting the *overt* data acquisition and communications systems. Fundamental questions however arise regarding the possibility of *covert* approaches for networking leading to breaches in both security and privacy. In this paper, we propose to study the possibility of, implications to and mitigation approaches for covert networking in the context of WVSNs.

III. SECURITY CHALLENGES

A. *Covert Channels and Steganography*

Covert channels exist in information systems that possess the following general characteristics: (1) shared resources, (2) redundancy, and (3) uncertainty. The shared resources enable communications to take place and the redundancy and uncertainty provide capabilities to hide the information transfer. Typically covert communications make use of system resources that are not normally used for communications; classical covert channels are known as either timing or storage channels. Thus, such mechanisms are often exploited to pass secret information discretely between two parties. Covert channels are typically identified and limited as much as possible to avoid unwanted information leakage from a trusted system component to an untrusted or less trusted component. Information leakage presents an important threat for any network. In such scenarii, corrupt system components can extract sensitive data from high security areas without raising alarm. WVSNs are easily attackable because they are often deployed in public areas where nodes can easily be accessed. Moreover, the collaborative nature of the ad hoc networking typical of sensor networks enables a single corrupted node to have unwanted effects on an extended part of the overall system. Figure 1 demonstrates how a stealthy malicious network can covertly exist atop of an existing overt and seemingly trusted network.

Figure 1 points demonstrates how an attacker can strategically corrupt physically accessible nodes to build his or her own covert overlay network. Due to the highly collaborative nature of networking and the need for shared resources, the attacker can have access to more information than the set of corrupted nodes originally provides. Additionally, WVSNs are of particular interest to attackers because they convey information as visual frames which are typically represented as large volumes of data. These images captured by every node, or camera, of the network represent a rich environment for hiding data to facilitate covert communication via the process of steganography.

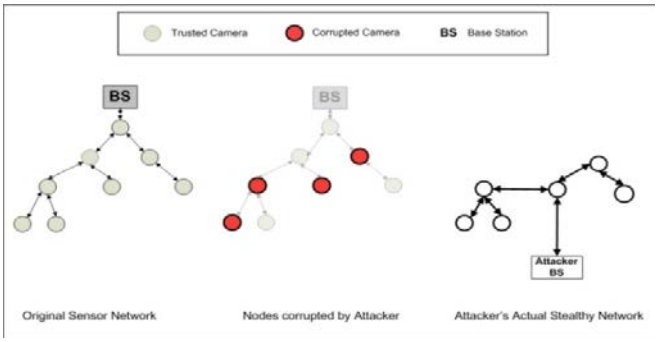

Fig. 1 Corrupt covert sensor network atop an original seemly trusted network

Steganography is the process of hiding covert information within other seemingly innocuous information called the host. Typical media types for host information are still and moving images. A simple steganographic system, as illustrated in Figure 2(a), involves two entities sharing information: the sender and the receiver. The sender can transmit data stealthily by hiding a message in an innocuous looking host image, for example. This embedding of information is commonly done via the use of a symmetric secret key K shared by both parties. The overt host information, which will be referred as *I*, is called the cover-media. The hidden information, denoted *W*, is also commonly referred as a watermark. After embedding the covert information W within the cover-media *I*, the resulting signal is called the stego-media, *I'*, and is typically identical in some "perceptual" senseto the cover-media hence making it difficult for another party to identify the occurrence of covert communications. For instance if the media represents still or moving images then the stego-image would have to be visually identical to the cover-image. The receiver can retrieve the hidden information W by means of the same key K used for the embedding. Because of the potential for covert communications in wireless sensor networks and their relative lack of defense against attackers, it is of importance to better understand the capabilities for and defense against covert activities.

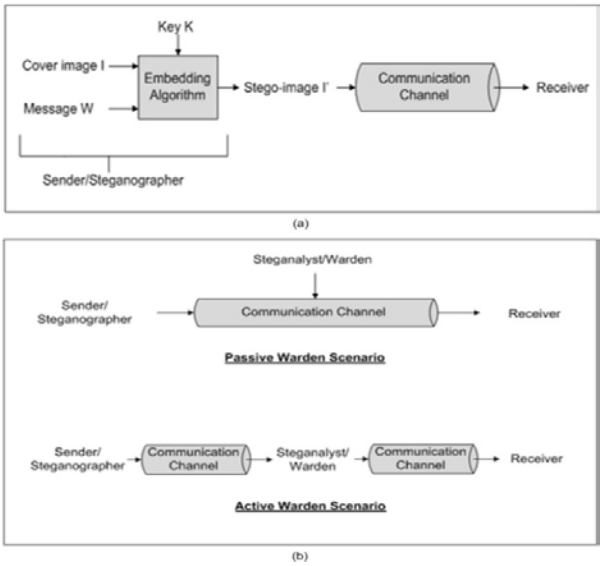

Fig. 2 (a) Steganographic system. (b) Active and passive wardens in steganalysis

B. Steganalysis

Steganalysis represents a defense against steganography by either identifying the presence of data hiding or limiting its possibility in a given system. Several classifications of steganalysis exist. Steganalysis can be reactive or proactive and it can involve an active or passive warden scenario as illustrated in Figure 2(b).

A proactive steganalysis solution is necessary when protection against a class of steganographic techniques is required. On the other hand, reactive steganalytic solutions target a specific steganographic embedding method. In an active warden scenario, the steganalyst acts as a middle man between the sender and the receiver of the stego-media. This implies that the warden is free to apply any data processing techniques to the covert-media before passing it to the actual receiver of the covert-communication. By doing so, the warden can deliberately transform the potentially corrupted host and as a consequence weaken or even eradicate the presence of steganography. In a passive warden scenario, however, the steganalyst can only eavesdrop on the communication between the two suspicious parties. The role of the steganalyst is therefore rather limited in the sense that it can only detect the presence of steganography but cannot prevent the covert-communication to occur. Thus, passive warden steganalytic solutions are often too restrictive to effectively defend against WVSN steganography. Active warden solutions may also be unsuitable for WVSNs because they usually require the use of lossy transformations in order to compromise the steganography which may raise questions as to the integrity of the WVSN information.

Therefore a grand challenge that arises is for the steganalyst to create an efficient solution against covert-communications that does not compromise the salient application-specific data content by effectively accounting for the specific architecture and goals of the network. Furthermore, it is possible that certain visual processing could serve to facilitate the intended overall WVSN goal, while ensuring to a high degree that any data formerly embedded or posthumously embedded will have a chance of detection by a steganalyst. We leverage this concept for preventative steganalysis.

The goal of preventative steganalysis is to provide protection against covert communications in WVSNs by ensuring that any potential cover-media within the network has statistical characteristics such that any previously hidden data has close to no chance of being undetected by a covert receiver and any possible future data to be hidden has limited opportunity to be communicated imperceptibly within that cover-media. Stated more specifically, the presence of steganography within the cover-media has a detection probability 1-ε. We strive to design solutions that make εapproach zero so that the steganalysis can reach ideal success rates thus discouraging any potential attacker from conducting data hiding.

IV. PROPOSED ALGORITHM

We first adopt a specific model for the images captured by the network. We initially restrict our study to the behavior of one single node N_i for simplification. To represent the entirety of the network, the process can then be extended on a node-by-node basis to the entire network. Node N_i is set to capture frames, noted *I'*, which are modeled as the sum of three different components or subframes as shown in Equation 1.

$$I' = W + D + B \tag{1}$$

where:

- *W* is the watermark,
- *D* is the critical data,
- *B* is the frame background,
- *W* and *B* maybe correlated,
- *W* and *D* are independent,
- *B* and *D* are independent.

A. Steganalysis Considerations

The definition of preventative steganalysis implies thatasimple analysis of the media *I'* gives as much information about the watermark *W* as possible such that the steganalysis can yield high success rates. This can be achieved by exploiting the uncertainty between *W* and *I'*, or more specifically, the uncertainty about *W* from the observation of *I'*. This quantity can be measured via the uncertainty coefficient as described in [10]. The uncertainty coefficient between two variables *X* and *Y* is defined as:

$$U(Y|X) = \frac{I(X;Y)}{H(Y)} \tag{2}$$

It quantifies the amount of knowledge about *Y* that can be derived from *X*. The uncertainty coefficient takes value between *0* and *1*. It achieves *0* when *X* and *Y* are uncorrelated and reaches *1* when *Y* can be entirely predicted from*X*.

In our case, we are interested in evaluating the watermark *W* with the knowledge of the potentially corrupted frame *I'*. This involves computing the uncertainty coefficient $U_1(W, I')$:

$$U_1(W|I') = \frac{I(W;I')}{H(W)} \tag{3}$$

Our goal is to make $U_1(W|I')$ as close to *1* as possible so that the most information about *W* can be obtained from *I'*. This can be achieved if we manage to build a frame *I'* in such a manner that the following equality can be obtained:

$$I(W;I') = H(W) \tag{4}$$

Equation 4 does represent the steganalyst's ultimate goal since from the derivation given by Equation 5, Equation 4 implies that the conditional entropy of *W* given *I'* is *zero*, i.e. the knowledge of frame *I'* leads to the perfect knowledge of the watermark. Under such circumstances, the watermark is clearly identifiable and no covert communication can occur undetected.

$$I(W;I') = H(W) - H(W|I') \tag{5}$$

B. Data Preservation

While it is of the utmost importance to provide a steganalytic cover for the network, it is at least equally

important that the WVSN can still perform its primary duty, whether it involves data mining activities or area monitoring. In other word, the steganalysis must not interfere with the integrity of the data *D* collected by the network. In other words, when data is present in frame *I'*, it is important that *D* can be easily and preferably entirely predicted with the observation of *I'*. This can be expressed with another uncertainty coefficient $U_2(D|I')$:

$$U_2(D|I') = \frac{I(D;I')}{H(D)} \quad (6)$$

Our goal is to make $U_2(D|I')$ as close to 1 as possible. $U_2(D|I') = 1$can be achieved if there exists a frame *I'* such that:

$$I(D;I') = H(D) \quad (7)$$

C. Common Solution

In order to develop a preventative steganalytic solution that will protect the network against covert communications and will keep the collected data intact, both Equations 4 and 7 must be satisfied. Therefore the steganalyst must find a common solution to the system:

$$findI'suchthat \begin{cases} I(W;I') = H(W) \\ I(D;I') = H(D) \end{cases} \quad (8)$$

Reasoning in two separate steps and using Equation 1, we first focus on the mutual information *I (W, I')* which can be further derived:

$$\begin{aligned} I(W;I') &= I(W;W+D+B) \\ &= H(W+D+B) - H(W+D+B|W) \\ &= H(W+B) + H(D) - H(D+B|W) \\ &= H(W+B) + H(D) - H(D) - H(B|W) \\ &= H(W+B) - H(B|W) \end{aligned} \quad (9)$$

For the previous equation to lead to the desired result offered by Equation 4, it is necessary to solve:

$$H(W+B) - H(B|W) = H(W) \quad (10)$$

This equality can be achieved in two trivial cases: when *W* and *B* are independent or when *B* is a known, temporally independent entity. On the case where*W* and *B* are independent, Equation 10 becomes:

$$\begin{aligned} H(W+B) - H(B|W) &= H(W) + H(B) - H(B) \\ &= H(W) \end{aligned} \quad (11)$$

Alternatively, if *B* is a known and temporally independent entity, *B* can be seen as a constant *Bc* for which we have:

$$\begin{aligned} H(W+B_c) &= H(W) \\ H(B_c|W) &= H(B_c) = 0 \end{aligned} \quad (12)$$

And Equation 10 would become:

$$H(W+B) - H(B|W) = H(W) \quad (13)$$

Both solutions are satisfying. However, assuming *W* and *B* are independent is not realistic and goes against our initial set of assumptions. The steganalyst should expect the attacker to use elaborate steganographic techniques where the steganography would not stand out in the background which implies a degree of correlation between *W* and *B*. Therefore, the solution where *B* is set as a known constant *Bc* is preferred.

Assuming that the background is a known entity such that $H(B_C) = 0$, we derive the second equality in Equation 8, i.e. the mutual information *I (D; I')*, which boils down to:

$$\begin{aligned} I(D;I') &= I(D;W+D+B_c) \\ &= H(W+B_c) + H(D) - H(W+B_c) \\ &= H(D) \end{aligned} \quad (14)$$

Equation 14 injected in Equation 6 gives an uncertainty coefficient $U_2(D|I')$ of 1 which by definition ensures that the data will remain identifiable when the frame *I'* is observed. Thus the substitution of the actual frame background *B* for a known and constant background *Bc* guarantees that the potential watermarking *W* appears more evidently in the frame *I'* and that the integrity of the data collected by the network is preserved.

V. IMPLEMENTATION

Let *Bk* represent the first frame captured by *Ni* during the calibration of the network. It is reasonable to assume that *Bk* is an untainted image free of steganography and critical data. Thus frame *Bk* is a perfect candidate to replace the actual background of any future visual recording.

The frames *I'* that node *Ni*records can now be decomposed into four components: the data, the watermark, the background and some noise. Therefore Equation 1 becomes:

$$\begin{aligned} I' &= W + D + B \\ &= W + D + B_k + N \end{aligned} \quad (15)$$

where:

- B_k is the reference frame,
- *W* is the watermark,
- *D* is the critical data,
- *N* is some noise corresponding to the difference between B_k and *B*.

In order for *I'* to be of the desired form $I' = W + D + B_c$, it is necessary for*N*to be removed from *I'*:

$$B_c = B_k \ and \ N = 0 \Rightarrow W + D + B_k + N = W + D + B_c \quad (16)$$

For illustration purposes, we use a sequence of surveillance of a child's playground. Figure 3(a) shows the frame which serves as the reference *Bk*. Figure 3(b) shows a random frame I' from the same sequence where the data D, i.e. the ball, has appeared.

To facilitate the denoising process, we can isolate *N* by subtracting *Bk* from *I'* so that only the noise and the data remain as illustrated in Figure 3(c) which shows the disparities between the actual background of *I'* and the reference frame *Bk*. The objective is to isolate the data and get rid of the other irrelevant discrepancies so that nothing left can negatively affect the steganalysis and *D* remains

intact. We try two solutions to achieve the suppression of *N* based on the same assumptions: the data covers a large block of connected pixels whereas the noise *N* is zero-mean and sparsely distributed over *I'*. These two solutions respectively involve a simple denoising filter and an area-based masking technique.

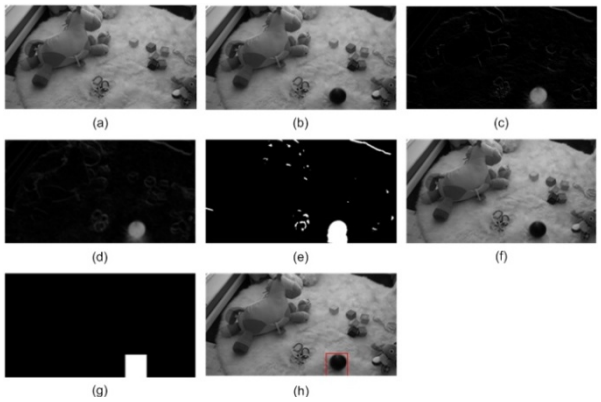

Fig. 3 Illustrations of algorithm.(a) Reference frame Bk,(b) Frame I' with intruder ball, (c) Frame difference Bk-I',(d) Average filtering ofBk-I', (e) Mask obtained after thresholding,(f) Reconstructed frame after filtering,(g) Mask from area-based technique,(h) Reconstructed frame from area-base algorithm with original data highlighted by rectangle

A. Average Filtering

Because *N* has the characteristics of a zero-mean noise, a simple denoising filter, e.g. an averaging filter, can at least considerably weaken *N*.

By filtering the frame difference *Bk-I'*, the data will of course be altered as well but as a large group of pixels of similar intensity, it will retain most of its shape after filtering whereas the rest of the smallest artifacts will mostly be erased. Figures 3(d) and 3(e) provide insight on the effect of using an averaging filter on the frame of Figure 3(c). As it can be seen, a great portion of the discrepancies present in Figure 3 (c) is erased whereas the data is still visible in Figure 3(e).

Figure 3(e) is used as a mask to reconstruct the final frame from Figure 3(f): black pixels in Figure 3(e) are replaced by pixels from the reference frame *Bk* and white pixels are preserved from the original frame *I'*.

Although the average filtering solution shows great results in this case, it is to be noted that depending on the size and shape of the data *D*, the denoising filter can have serious consequences on the integrity of *D*. For example, a square shape will become rounder with the use of an averaging filter. And although the network will probably still flag the presence of data in *I'*, it might be more difficult for the user to identify the true nature of the data.

B. Area-Based Alternative

In order to avoid the problems that can be encountered with a filtering technique, we also try using analternative technique based on area selection. This solution works in such a way that large clusters of connected pixels emerging from the difference *I'-Bk* are protected whereas the rest of the difference is cleared of any interferences by setting all unprotected pixels to black.

Figure 3(f) shows the mask obtained after the area selection algorithm has been applied to the frame in Figure 3(c). In this case, the white rectangle shows that the area containing the large group of light pixels is the only remaining part of the original frame. As for the previous algorithm, the black pixels in Figure 3(f) are replaced by pixels from *Bk* and white pixels are replaced by pixels from the original *I'* frame. The result of this area-based technique is shown in the reconstructed frame of Figure 3(g). A rectangle is drawn around the area containing the original pixels from *I'* which clearly proves that the area surrounding the object constituting the data remains.

This method is more efficient in getting of any potential discrepancy between the actual frame background and the reference one *Bk*as shown in Figure 3(f). However, depending on how precise the selection of the concerned area is, the number of protected, or masked, pixels that do not belong to the data *D* varies. For example, Figure 3(g) indicates that a portion of the original frame inside the marked rectangle, although not part of the data *D* itself, manage to find its way in the reconstructed frame unchanged. In case the area masked is of large proportions, more noise might go through the cleaning process untouched. This could therefore diminish the efficiency of the preventative steganalysis.

C. Common Outcome

In both cases, after processing, the steganalyst expects to find *I'* to be as close as possible as being the sum of only three parts:

$$I' \approx W + D + B_k \quad (17)$$

From this equality, it is clear that in the absence of watermark, the isolation of the data *D* becomes an easy task as *Bk* is a known entity. When steganography has occurred, because *W* and *D*habe different distribution and *Bk* is known, the preventative steganalysis is expected to yield high success rates.

VI. SIMULATIONS

To assess the validity of the proposed algorithm as a working proactive steganalytic system, several experiments are conducted. These experiments include:

- Simulations on the uncertainty coefficient,
- Simulations on data preservation,
- Simulations on steganography detection.

The simulations are conducted on a series of sequence of frames showing a child's playground shown in Figure 3(b). In this setting, the goal of the network is to detect the presence of a ball in the playground by identifying round objects in the frame.

A. Uncertainty Coefficient $U_1(W|I')$

$U_1(W|I')$ is computed for watermarked sequences where *W* is an additive white Gaussian noise. Tests are conducted on unprocessed sequences first, then on the same sequences when the actual background is replaced by the reference background *Bk*. The tests are also conducted on the

sequences derived after the filtering process and the area selection technique have been applied after the background has been substituted for Bk. The watermark is embedded with a signal-to-noise ratio of 20 dB relative to the image.

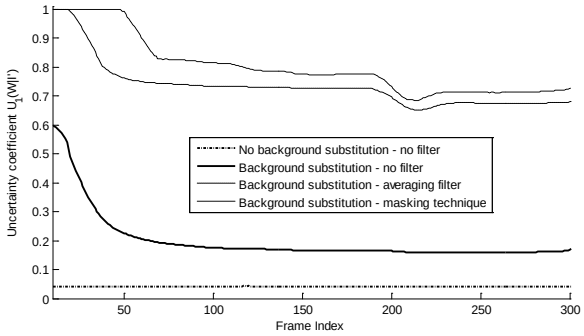

Fig. 4 Uncertainty coefficient for frame sequence at various stages of processing with a watermark embedded with a SNR of 20dB

Figure 4 shows that our proposed solution is effective in increasing the uncertainty coefficient $U_1(W|I')$ eventually making the watermark more easily detectable. When the actual background is replaced with *Bk*, it logically appears that the first frames in the sequence obtain the highest uncertainty coefficient due to the higher correlation with *Bk*. The uncertainty coefficient gets lower with time which can be explained by the appearance of the relevant data D in the frame and the eventual perturbation of the scenery has time goes by. This suggests that improvement could be achieved if the reference frame was refreshed at different points in time.

Overall, the computation results for the uncertainty coefficient $U_1(W|I')$ provide proof that the derived algorithms can greatly improve the knowledge of the steganalyst on the potential presence of watermarking.

B. Data Preservation

Although the primary objective of the steganalyst is to protect the network against covert communications, the steganalysis must not interfere with the network's main objective. In monitoring applications, the network collects critical data which must still be identifiable after the steganalysis has taken place.

To quantify the effects of the steganalysis on the data, we test the efficiency of a data detection algorithm with the unmodified frame sequence and after our proposed solution has been applied.

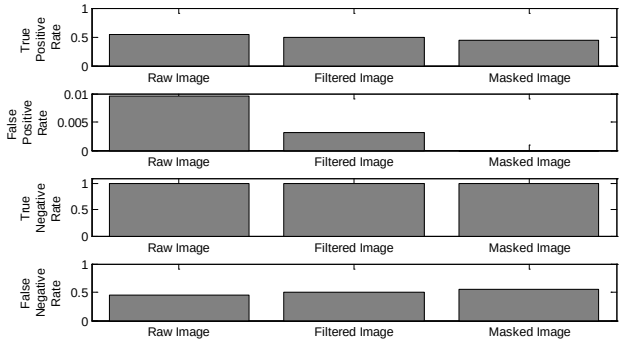

Fig. 5 Data detection outcomes for uncorrupted frame sequences

Figure 5 shows the success and error rates of the algorithm used to detect the presence of round objects. The results are drawn in the case where no steganography has occurred since purely the effects on the data are desired. What we are interested in is not the efficiency of the detection algorithm itself but rather in the changes in the detection outcome after the use of our proposed steganalytic solution. The results show a slight decrease in the rate of true positives but an important decrease in the rate of false positives. The results also show a rather similar true negative rate and a slight increase in the rate of false negatives. From these results we can infer that the data identification algorithm performs as well in each situation. Although the critical sensibilityis slightly decreased, the specificity of the detection is improved. It is to be noted that parameters in the steganalytic solutions can be tweaked to find the best compromise between steganalytic protection and data preservation depending on the desire of the network's users.

C. Steganography Detection

Because steganalysis is about protecting the sensor network against the possibility of covert communication, it is necessary to evaluate how well the preventative steganalysis performs. In order to verify if our preventative steganalytic approach leads to high success rates a simple threshold-based detector is derived. In this paper, we use an average block variance threshold-based detector.

The detector computes the average variance of blocks of pixels from the frame *I'*. Each frame is divided in a certain number of blocks where the variance is computed. The block variances obtained are then averaged over the whole frame. A block-based algorithm is suggested in order to reduce the effect that the presence of data might have on the final steganalytic decision. For example, if the steganalyst was to count the number of pixels originating from image aberration, the data *D*, as a large group of pixels, would have a great influence on false positive rate of the detector decision.

Frames are chosen randomlyand corrupted with an additive white Gaussian watermark in both sequences obtained after the steganalytic solutions proposed have been applied to the original sequence. For the fairness of comparison, the same frames in both sequences are corrupted with identical watermark. The embedding is done using a signal-to-noise ratio of 30dB with regards to the original image. Computations of the average block variance are derived and presented in Figure 6.

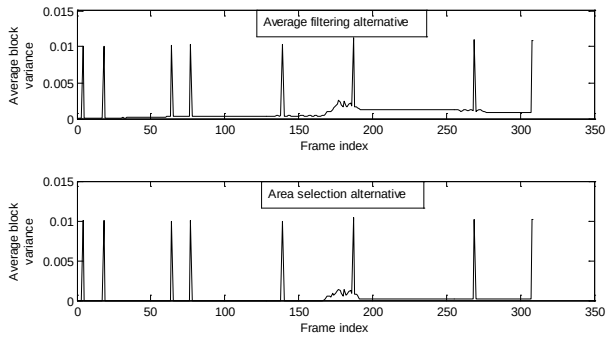

Fig. 6 Average block variance in corrupted processed sequences

Figure 6 shows similar results for both derived solutions. In presence of a watermark the computation of the average block variance leads to an important increase in value. The presence of data, mostly visible from frame 170 to 200 in Figure 6, also creates an increase in the computed variance but in a different scale than watermarking does therefore confusion between the presence of data and the presence of watermarking is unlikely.

Computing the ratios of the obtained variance extrema shows that when with the averaging filter solution, the presence of watermarking increases the average block variance by a *2e+4*factor, whereas for the area-based solution, this factor increases to *5e+4*, thus concluding that the area-based solution leads to better steganalytic results.

VII. CONCLUSION

In this paper we have discussed the problem of defenses against covert communications in visual sensor networks. Because of the critical purpose of a WVSN, precautions have been implemented to insure the integrity of the data collected by the network's cameras. Solutions providing both protection against steganography and against data corruption have been presented and their efficiency discussed through several simulations. Results from the simulations proved that the detection of steganography is made easier for the steganalyst while the data identification algorithm still performs well.

While promising, preventative steganalysis obviously needs to be investigated further. Preventative solutions imply that the processing of the information needs to be done early on in the chain of node communication. It would be interesting to assess the effect of such solutions on already corrupted frames. By doing so, we might find out preventative steganalytic solutions would not imperatively need to be applied at the capturing node to ensure protection against steganography. It is also important to develop customized solutions adapted to the specifics of the network such as its function, its size and its available resources in order to increase the efficiency of the steganalysis.

REFERENCES

[1] B.P.L. Lo, J.L. Wang, and G.-Z. Yang, "From imaging networks to behavior profiling: Ubiquitous sensing for managed homecare of the elderly", *Adjunct Proceedings of the 3rd International Conference on Pervasive Computing*, Munich, Germany, pp. 101–104, May 2005.

[2] D.A. Fidaleo, H.-A. Nguyen, and M. Trivedi, "The networked sensor tapestry (NeST): A privacy enhanced software architecture for interactive analysis of data in video-sensor networks", *Proceedings of the ACM 2nd International Workshop on Video Surveillance & Sensor Networks*, New York, USA, pp. 46–53, October 2004.

[3] J. Wickramasuriya, M. Datt, S. Mehrotra and N. Venkatasubramanian, "Privacy protecting data collection in media spaces", *Proceedings of the 12th annual ACM International Conference on Multimedia*, New York, USA, pp. 48–55, October 2004.

[4] D. Kundur, W. Luh, U.N. Okorafor, and T. Zourntos, "Security and Privacy for Distributed Multimedia Sensor Networks", *Proceedings of the IEEE Special Issue on Distributed Multimedia*, vol. 96, no. 1, pp. 112-130, January 2008.

[5] J. Feng, M. Potkonjak, "Security in sensor networks: watermarking techniques", *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents V*, vol. 5020, pp. 391-402, June 2003.

[6] J. Zheng, J. Li, M. J. Lee and M. Anshel, "A lightweight encryption and authentication scheme for wireless sensor networks", *International Journal of Security and Networks*, vol. 1, Issue 3, pp. 138-146, December 2006.

[7] I. Martinovic, P. Pichota and J. B. Schmitt, "Jamming for Good: A Fresh Approach to Authentic Communication in WSNs", *Proceedings of the Second ACM Conference on Wireless Network Security*, Zurich, Switzerland, pp. 161-168, March 2009.

[8] E. Blaß, J. Wilke and M. Zitterbart, "Relaxed authenticity for data aggregation in wireless sensor networks", *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, Istanbul, Turkey, pp. 1-10, September 2008.

[9] J. Jainsky, D. Kundur, and D. Halverson, "Towards digital video steganalysis using asymptotic memoryless detection", *Proceedings of the 9th Workshop on Multimedia & Security*. Dallas, TX, USA, pp. 161-168, September 2007.

[10] W.H. Press, S.A. Teukolsky, W.T. Vetterling and B.P. Flannery, *Numerical Recipes: The Art of Scientific Computing (Second Edition)*, Cambridge, UK: Cambridge University Press, 1992.

Julien S. Jainsky received his engineering degree in electrical and computer engineering in 2005 from CPE Lyon in France. He is currently a Ph.D. candidate in the Wireless Communication Group (WCL) of the Department of Electrical and Computer Engineering at Texas A&M University under the advisorship of Drs. DeepaKundur and Don Halverson. His research interests include security in multimedia, sensor networks and smart grids.

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering in 1993, 1995, and 1999, respectively, from the University of Toronto, Canada. From September 1999 to December 2002 she was an Assistant Professor and held the title of Bell Canada Junior Chair-holder of Multimedia in the Department of Electrical and Computer Engineering at the University of Toronto. In January 2003, she joined the Department of Electrical and Computer Engineering at Texas A&M University, where she is currently an Associate Professor.

She is the author of over 100 technical publications in the field of information security, multimedia and signal processing and communication systems. Her research interests include cyber security of the electric smart grid and security of multimedia sensor networks. She is an appointed member of the NERC Smart Grid Task Force and an elected member of the IEEE Information Forensics and Security Technical Committee.