Enhancing the Security of a Gateway through Steganography

Docas Nwanebu
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
dnwanebu@csir.co.za

Abstract- Securing information is a paramount feature in the world of internet where there is consistence enormous flow of information. With everyone having access to the same internet, sensitive information needs concealment from adversaries. Especially in an environment like the military, information confidentiality and data integrity in a tactical communication network is a priority. A gateway is a technology developed for the South African Defence Force (SANDF) for achieving interoperability between SANDF static and tactical communication networks; the gateway provides a common information communication model for the transmitting of video, voice and data between different communication networks. In this paper, we study the enhancement of security measures between gateways deployed in a tactical network with respect to video streaming. Ongoing research has proven that steganography combined with existing encryption techniques can provide increased security. Steganography is a technique used to conceal the existence of information from detection by unauthorized users. A focus of this study is on video steganography techniques with respect to the measurement of the performance metric namely level of security. A theoretical comparison of the findings from this survey is discussed and the best suitable method for the gateway is presented.

Keywords: Gateway, video, streaming, steganography, encryption, tactical network.

1. Introduction

Steganography in its basic form means covered writing. It is simply a means of concealing the very existence of information. (Abomahara, et al., 2015) The main goal of steganography is to communicate without any intruder suspecting that there is in fact communication. (Challita & Farhat, 2011)
Steganography uses a cover or carrier (media file) such as an audio, image or video to cover or hide a secret message (media file). A media file could be an image, audio, or video or text. (Lindawati & Siburian, 2017)

Unlike steganography, cryptography scrambles information so that, it is unreadable to the human eye. With cryptography attackers know that there is information existence but cannot read it (Yadav, Mishra et al. 2013) Extensive research has been going on for a while on cryptographic techniques and has proven to protect information to an extent. With the world of communication, moving from pen and paper to mostly digital, more robust communication systems needs enhancement. With that said, cryptography alone may not serve the purpose of secret communication, but cryptography combined with steganography can provide more robustness to communication systems. Although no steganography or cryptography technique guarantees hundred percent security from attackers, but the combination of the two means if for example steganography fails, the attacker still has to break the cryptography algorithm to get to the encrypted message. (Laskar & Hemachandran, 2012)

A gateway is a technology developed for the SANDF to serve as a communication bridge between all systems in a tactical network. It provides protocol conversion such that systems that would not communicate with each other because of different protocols will end up interoperable across the tactical network. (Duvenhage & Terblance, 2008) The gateway in addition to voice and data has also integrated video, which means that military personnel can also use live streaming to communicate or replay stored videos. If different entities in the world use steganography and cryptography to secure sensitive information, how much more is a high profile department like the military? Therefore, this paper presents a review of steganography techniques and presents a most secured technique for the gateway.
The rest of the paper is as follows: Section 2 presents the related work in the field of steganography, Section 3 discusses the implementation of steganography on the gateway, Section 4 concludes the paper and Section 5 presents the future work.

2. Literature Review

Video steganography on a video simply means using a video to hide another video i.e. one video is the cover file and one video is the secret video. A stego-video is the combination of a cover (carrier) video embedded with a secret video. (Patel & Patel, 2014) Figure 1 depicts the art of steganography with respect to video, here the secret video is concealed into a carrier file(video) through a steganography algorithm to form a stego-video file. The stego-video is transmitted through the internet to its intended receipent, prior to its arrival, the extraction algorithm then separates the secret video from the carrier video.

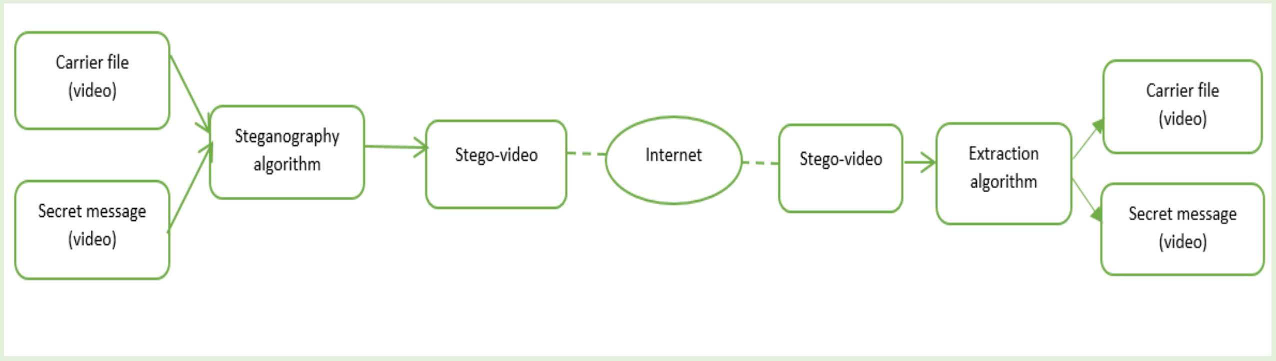

Figure 1 Overview of video steganography

2.1 Least Significant Bit based Steganography

The Least Significant Bit (LSB) method is one of the widely used technique because of its simplicity to implement. The LSB method simply converts an image into bits, separate the least significant bits from the most significant bits of the image and substitute the least significant bits with the secret message. (Hussain & Hussain, 2013) It is also known as a substitution-based spatial domain method because of the substitution of bits, spatial domain refers to the image itself in pixels. (Bhattacharyya, et al., 2011) Quiet extensive research occurred over the years on steganography techniques using the LSB method. Many on image and audio but lately video steganography is immensely gaining momentum because of the large space available to hide data. (Abomahara, et al., 2015) Video is a combination of still images with a sound, thus the same methods used for image steganography can work on video too. (Yadav, et al., 2013) The difference with hiding a video in another video is that a video has many images to hide, while in image steganography there is only one or two images to hide. Thus, video steganography may be very complex to implement and may have added computational complexity than hiding one image.

Patel & Patel(2014) implemented steganography using the LSB method. The research implements video steganography combined with encryption. Video frames are used to hide a secret video in avi format. The secret video is divided into frames, grouped into sizes of RxC where R is the length of row pixel and C is the length of Column Pixel. The secret video is rearranged to conform to a specific pattern, encrypted and concealed in the LSB of the image of the video cover. According to the researchers, the performance results of the algorithm showed a zero bit error rate of the hidden message, meaning no bits were lost during the hiding and extracting of the secret video. However, the video is an uncompressed avi format, and transmitting video uncompressed means large bandwidth consumption.

Yadav, Mishra et al. (2013) has done similar work by using video as a cover file to hide a video as the secret message. The algorithm combined symmetric key encryption and video steganography based on the LSB. Robustness of the algorithm was determined by the level of imperceptibility of the video that embeds the secret video, and the validity of the extracted secret message from the stego-video. Peak Signal to Noise-Ratio (PSNR) and Root Mean Square Error (RMSE) were the performance metrics used to measure the level of imperceptibility and validity. Imperceptible means that the embedded carrier video (stego-video) must be similar to the original carrier video and validity means the embedded secret video must be similar to the original secret video. The results illustrated no visual distortion to the carrier video and the recovered secret video was acceptable.

Researchers (Solichin & Painem, 2016) conducted work on video steganography using the LSB in conjunction with the Least Significant Frame (LSF) to hide a secret text document in a video file. The proposed method selects the least significant frame based on optical flow features. The secret document is concealed in the least significant bit of the selected least significant frame. The outcome proved the LSF method to have a better stego-video quality based on PSNR values than without LSF.

2.2 Transform Domain based Steganography

Transform domain techniques on steganography has been an active field of research on image processing. Though known to be a cumbersome technique to implement compared to the LSB techniques, research has proven their ability to provide more robustness and improve imperceptibility. (Hussain & Hussain, 2013)
Transform domain techniques transforms the spatial domain of a cover file (media) into a frequency domain, and the resultant transformation is called a coefficient. The secret message is embedded in the least significant bits of the coefficient. (Yadav, Mishra et al. 2013) Commonly used transform domain techniques in steganography are the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

DCT method transforms an image or signal from spatial domain to frequency domain. The DCT algorithm transforms an N x N pixel block of an image into two-dimensional N x N coefficients. The resultant coefficient clearly displays the low, mid and high frequencies. The transform coefficient of an N x N image pixels are computed by function *F(x,y)* where *x* and *y* is the row and column position of each pixel. The inverse of function *F(x,y)* is used to restore the image back to spatial domain. The low frequencies contains the essential visual part of an image and that is where much of the signal strength lies, whereas high frequencies are known to have small values that can be easily compressed or used to hide secret messages with little visual distortion to the human eye. (Vaishali & Bhat, 2015) (I-Ming P, 1999)

DWT hierarchically decays an image into small waves known as wavelets. (Vaishali & Bhat, 2015) (Walia & Jain, 2010) DWT method is advantageous over DCT because of its ability to capture frequency and location information. The algorithm breaks down the image into multi-resolution sub-bands known as lower approximation (LL), horizontal (HL), vertical (LH) and diagonal components (HH). The HH components is a high frequency sub-band, which is the perfect location to embed a secret message. (Sharma & Kumar, 2013)

Sharma & Kumar (2013) conducted a study of image steganography using both DCT and DWT. The authors measured the performance of these techniques based on PSNR, Mean Square Error (MSE), robustness and capacity. The DCT method achieved high quality of the image based on the high PSNR value attained, while the DWT method showed to be a more robust algorithm than DCT against image manipulation by hackers.

Yang & Bourbakis (2005) proved that DCT transform steganography techniques can be applied successfully even to lossy compression video codecs such as H.246/AVC. In this research, the implemented algorithm divides the DCT 4x4 coefficients into sub-blocks and hide secret information into low-frequency sub-blocks. The algorithm is first applied and then the stego-video is compressed to H.264/AVC. The Bit Error Rate (BER) and PSNR were the performance metrics used to evaluate the algorithm. Results verified that high level of robustness was attained with no distortion to the image quality.

3. Comparisons of steganography techniques

Based on the reviewed literature, this section presents a comparison of the features of spatial domain technique (LSB) over transform domain techniques (DCT/DWT) as depicted in Table 1:

Table 1

	Least Significant Bit (LSB)	**Discrete Coefficient Transform (DCT)**	**Discrete Wavelength Transform (DWT)**
Algorithms	*Algorithm to embed message:-*	*Algorithm to embed message:-*	*Algorithm to embed message:-*

	Step 1: Read cover image and secret message which is to be hidden Step2:Convert secret message in binary Step 3:Calculate LSB of each pixels of cover image Step 4:Write the stego file *Algorithm used to extract secret message:-* Step 1: Read the stego file Step 2: Calculate LSB of each 8 bit into character Step 3: Retrieve bits and convert each 8 bit into character	Step 1: Read cover image Step 2: Read secret message and convert it to binary Step 3: The cover image is broken down into 8x8 block of pixels Step 4: Operating from left to right and top to bottom, subtract 128 in each block of pixels. Step 5: Apply DCT to each block Step 6: Compress each block through quantization table. Step 7: Calculate LSB of each DCT coefficient and replace with each bit of secret message. Step 8: Write stego file. *Algorithm used to extract secret message:-* Step 1: Read stego file Step 2: Stego file is broken into 8x8 block of pixels Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels. Step 4: Perform DCT to each block. Step 5: Compress each block through quantization table. Step 6: Calculate LSB of each DC coefficient. Step 7: Retrieve and convert each 8 bit into character.	Step 1:Read cover image and secret image Step 2: Convert the cover image using DWT to get approximated and detailed coefficients. Step 3: Choose one coefficient as the cover image. Step 4: Hide the secret message in the least significant bit of the cover image using the LSB embedding algorithm. *Algorithm used to extract secret message:-* Step 1: Read the stego file Step 2: Calculate the inverse of DWT Step 4: Retrieve the secret message from the LSB of the cover file
Robustness	Low	High	High
Hiding Capacity	High	medium	medium
Perceptual Transparency	Low	High	High
Peak Signal to Noise Ratio(PSNR)	Low	medium	High
Attack Schemes	The LSB method fails when a video is compressed with a lossy compression; this result in hidden information loss. Converting the file for instance from an avi	Lowering the bitrate results in codecs removing frequencies that are unheard by the human ear. Missing frequencies leads to loss of some parts of the	Lowering the bitrate results in codecs removing frequencies that are unheard by the human ear. Missing frequencies, leads to some parts of the

	to an rgb format will result in hidden message lost.	embedded message.	embedded message lost.
Advantages	Capable of hiding huge amount of data. LSB method is easy to implement, hence this makes the extracting process straightforward. There is minimal degradation of the of the stego file.	High compression rate, small bit error rate and good information integration ability. Method can be adapted to compressed video formats.	High bit rate data hiding method. Computational efficient. Method can be adapted to compressed video formats. Can break down an image into frequency and time domain.
Disadvantages	Not resistance to video manipulation and compression. Non-resistant to statistical attacks.	Computational complexity	Computational complexity

4. Steganography on the Gateway

4.1 Parameters of Evaluation

Figure 2 illustrate the parameters used to evaluate a steganography algorithm:

- *Security* – High security means the stego-video must be highly imperceptibility. The stego-video must not be any different to the original carrier video. It must maintain high quality to ensure that it is unsuspicious to attackers. This is accomplished by comparing the quality of the stego-video with the original cover video. Metric used mostly to determine perceptual transparency is the Peak Signal to Noise Ratio (PSNR). A high PSNR value means high quality image. (Vaishali & Bhat, 2015) (Sharma & Kumar, 2013)
- *Robustness*
    a. *Due to video compression* – when communicating through video, compression is necessary to save bandwidth. The hidden video stream with the carrier video must survive after codec compression. The Bit Error Rate (BER) can determine the number of bits of the secret message that survived and extracted successfully from the stego-video. (Abomahara, et al., 2015) This can show if the secret message survived the compression or not.

    b. *Due to image/video manipulation* – The algorithm should stand the test of manipulation from video processing such as addition or deletion of frames. BER tests can determine the ratio of the bits lost, this analysis can assist in knowing if the stego-video survived manipulation or not.

- *Hiding capacity* –Refers to the number of bits on an image available for hiding secret data. Video contains a huge amount of still images; this means a suitable algorithm must have sufficient capacity to hide many images.

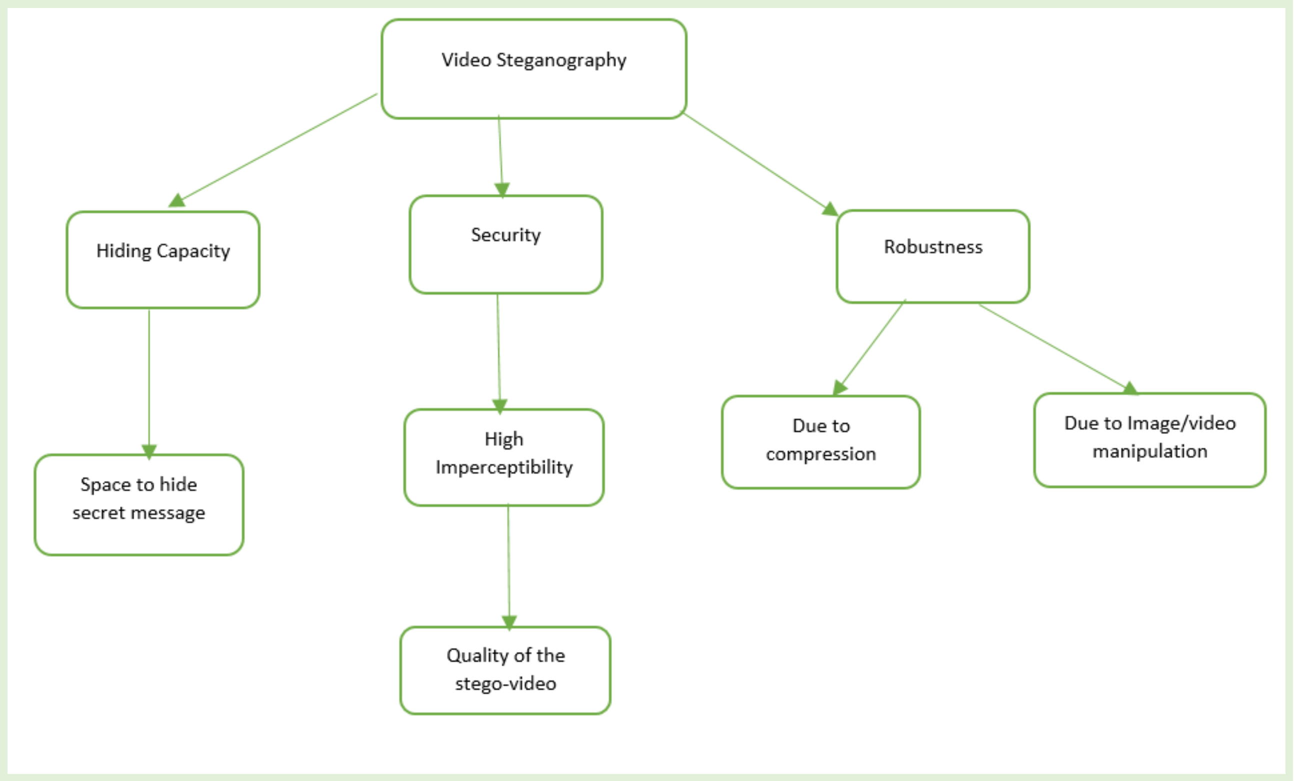

Figure 2 Ideal video steganography method

Videos are mostly in compressed format because a video stream is very large and to save bandwidth video compression is necessary. Research has substantiated that LSB based steganography techniques do not work well with compressed videos because of the least significant bits used to hide the secret information. (Hussain & Hussain, 2013) This is because if the stego-video is compressed the least significant bits that contains the embedded secret data may be lost. Therefore, for the implementation of steganography on the gateway, transform domain techniques stand to be suitable for the intended deployment

4.2 Deployment of Steganography on the Gateway

The gateway uses a framework for live image transformation called Flitr that enables live streaming video and capturing images from connected video sources. Flitr handles the image processing in the gateway. Figure 3 depicts the desired implementation of steganography and encryption, here the source device is any input device that has a camera and can send video to the receiving device. A receiving device is a web-based application used to receive incidents happening in a tactical field. With this receiving device, military personnel can use this application to play back stored videos or live stream. Gateway A will execute steganography and encryption from the source device and Gateway B will handle the extraction of the stego-video and decryption at the end before transmission to the receiving device. The addition of steganography on the gateway guarantees double secured communication channels in a tactical network.

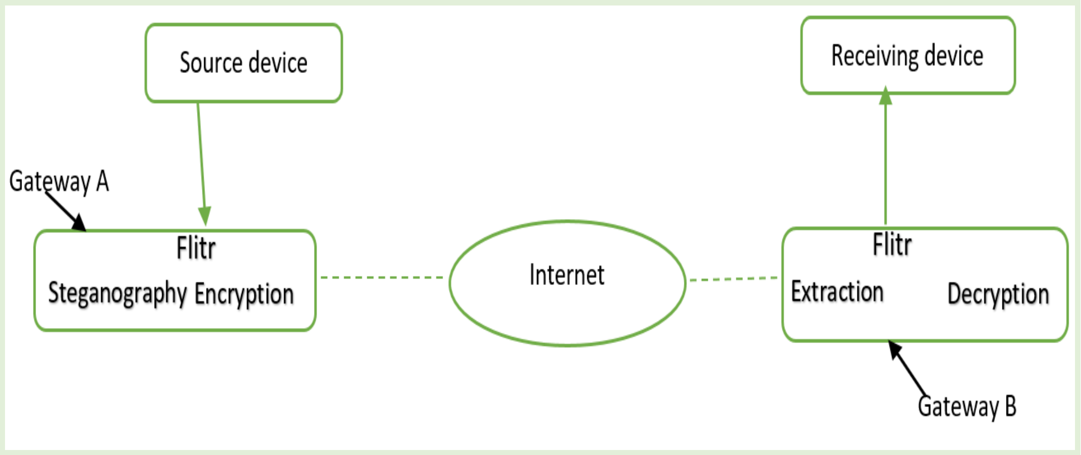

Figure 3 Deployment of steganography and encryption on the gateway

5. Conclusion

Steganography can provide security even better when combined with encryption. This led to the idea of implementing video steganography to a gateway deployed for the military. In this paper, the author presented a review study of related work on video steganography, presented a comparison of spatial and transform based steganography methods from literature analysis, and outlined the deployment scenario of steganography on the gateway. In conclusion, the closer the BER is to zero the more secure is the algorithm. The higher the PSNR the higher the imperceptibility of the secret message. A perfect steganography technique in reality does not exist; they all have pros and cons. However, transform domain DWT/DCT methods are thus far fitting methods for the gateway because of their many advantages over most commonly used LSB spatial domain technique. The main disadvantage of transform domain techniques are their complexity to implement, but their robustness to attacks appropriates them for the gateway.

6. Future Work

Firstly will be to conduct research on steganalysis schemes i.e. a study of techniques used by attackers to defeat steganography. Knowing these attacking schemes will assist in developing test scenarios for the selected steganography method. Secondly, a research on computational complexity of the transform domain techniques with respect to bandwidth utilization needs further study. Lastly, there are newer techniques of steganography such as adaptive transform domain techniques that needs exploration. Knowledge of these techniques may lead to a discovery of a more secure algorithm for the gateway.

7. References

Abomahara, M., Z, O. & K, O., 2015. Video steganography: a comprehensive review. *Multimedia Tools and Applications,* 74(17), pp. 7063-7094.

Abomhara, M., Zakaria, O. & Khalifa, O. O., 2010. An Overview of Video Encryption Techniques. *International Journal of Computer Theory and Engineering,* 2(1), pp. 1793-8201.

Bhattacharyya, S., Banerjee, I. & Sanyal, G., 2011. A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier. *Journal of Global Research in Computer Science ,* 2(4).

Challita, K. & Farhat, H., 2011. Combining Steganography and Cryptography: New Directions. *International Journal on New Computer Architectures and Their Applications ,* 1(1), pp. 17-24.

Dasgupta, K., Mandal, J. K. & Dutta, P., 2012. Hash Based Least Significant Bit Technique for Video Steganography (HLSB). *International Journal of Security, Privacy and Trust Management (IJSPTM),* 1(2).

Duvenhage, A. & Terblance, L., 2008. *The Evolution of a C2 Protocol Gateway.* Scotland, European Simulation Interoperability Workshop.

Hussain, M. & Hussain, M., 2013. A Survey of Image Steganography Techniques. *International Journal of Advanced Science and Technology,* 54(113-124).

Laskar, S. A. & Hemachandran, K., 2012. High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems,* 4(6), pp. 57-68.

Lindawati & Siburian, R., 2017. *Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio.* s.l., IEEE.

Patel, R. & Patel, M., 2014. *Steganography over video file by hiding video in another video file, random byte hiding and LSB technique.* s.l., IEEE.

Sharma, S. & Kumar, U., 2013. Review of Transform Domain Techniques for Image Steganography. *International Journal of Science and Research (IJSR),* 4(5), pp. 194-197.

Shou-Dao, W., Chuang-Bai, X. & Yu, L., 2009. A High Bitrate Information Hiding Algorithm for Video in Video. *International Journal of Computer, Electrical, Automation, Control and Information Engineering,* 3(11).

Solichin, A. & Painem, 2016. *Motion-based less significant frame for improving LSB-based video steganography.* s.l., IEEE.

Vaishali, P. & Bhat, P., 2015. Transform Domain Techniques for Image Steganography. *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING,* 3(1).

Walia, E. & Jain, P., 2010. An Analysis of LSB & DCT based Steganography. *Global Journal of Computer Science and Technology,* 10(1), pp. 4-8.

Yadav, P., Mishra, N. & Sharma, S., 2013. *A secure video steganography with encryption based on LSB technique.* s.l., IEEE.

Yang, M. & Bourbakis , N., 2005. *A high bitrate information hiding algorithm for digital video content under H.264/AVC compression.* s.l., IEEE.