High Volume Secure Data Hiding In Video

Asad Amir Pirzada
Raja Iqbal

School of Computer Science & Software Engineering
The University of Western Australia
e-mail: pirzada@csse.uwa.edu.au

College of Signals
National University of Sciences and Technology, Pakistan
e-mail: rajamcs@yahoo.com

Abstract

This paper proposes a Multi-Stream Cipher Steganographic technique for high volume and secure data hiding in digital video and images. The proposed technique enables high rate of data embedding along with provisioning of confidentiality, integrity and authenticity security services. Embedding is carried out in spatial domain utilizing multiple stream ciphers for embedding signature information. Signature data is first processed using an advance symmetric cipher. The cryptogram thus obtained is then spread over the individual colour bands of each pixel of every video frame using multiple cryptographically secure pseudorandom bit generators. This results in an extremely secure, imperceptible and alteration detectable steganographic scheme supporting high volume data embedding including picture-in-picture and video-in-video. An analysis of the proposed scheme against available steganalysis methods has also been carried out.

Keywords

Information Security, Cryptography, Steganography, Pseudorandom bit generators

1. INTRODUCTION

The need to establish secure imperceptible channels for secret communications and the ease of creating identical and illegal digital data prompts the need to establish reliable and secure methods for data hiding, copyright protection and verification. Multimedia data exposes a novel avenue for invisible and secure communication channels using digital cryptography and steganography. While cryptography aims at making data unintelligible for its viewer, steganography aims at concealing the very existence of presence of data. However, in practice a hybrid of these two schemes is utilized to attain both unintelligibility and concealment.

The requirements of any data hiding system can be categorized into security, capacity and robustness Cox et al. (1996). All these factors are inversely proportional to each other creating the so called data-hiding dilemma. The focus of this paper aims at maximizing the first two factors of data hiding i.e. security and capacity coupled with alteration detection. The proposed scheme is a data-hiding/hidden-communication steganographic method that uses digital video as a cover signal. The scheme is blind, as the original cover signal is not required to recover the hidden information. The proposed recipient need only possess the required keys in order to reveal the message; otherwise the very existence of the hidden information is virtually undetectable. The proposed scheme provides the ability to hide a significant quantity of information making it different from typical data hiding mechanisms because here we consider applications that require significantly larger payloads like video-in-video and picture-in-picture.

The following terminology is used in this paper. The signature or message data is the data that is being embedded or concealed. The source data is used to hide the signature data often referred to as the host data or cover. A signature hidden in the host is called the embedded data. The recovered data, also referred to as the reconstructed data, is the signature that is extracted from the embedded data. The payload capacity in data hiding indicates the total number of bits hidden and successfully recovered by the stego-system.

The paper is organized as follows. In Section 2 a review of related previous work has been carried out. Section 3 explains the working of the proposed scheme. In Section 4, an analysis of the performance and capacity of our proposed scheme has been discussed and in Section 5 we evaluate our scheme against available steganalysis techniques. Concluding remarks are presented in Section 6.
2. PREVIOUS WORK

Spread spectrum steganography is one of the earliest techniques for watermarking as proposed by Cox et al. (1997) and Marvel et al. (1999). It targets at distributing the message or signature information over a wide range of frequencies of the host data. Discrete cosine or the discrete wavelet transform coefficients are also utilized to embed the signature data. While much of the early work was on watermarking image data Hartung et al. (1997), Qiao et al. (1998), Tao et al. (1997), recently a number of methods have been proposed for implanting audio and video information in video sequences. Swanson et al. (1997) proposed an algorithm to hide compressed video and audio data into video. The message data is embedded in the DCT domain, by changing the projections of the 8x8 host block DCT coefficients. The data-hiding rate is two bits per 8x8 block. The authors demonstrate robustness to additive Gaussian noise and motion JPEG compression. Mukherjee et al. (1998, 2000) and Chae et al. (1999) present methods for data hiding in video using multidimensional lattice structures with data hiding rates of about 1%. Least Significant Bit (LSB) encoding directly substitutes the cover LSB with the message bits by means of some type of logical or arithmetic procedure. Numerous examples of LSB schemes have been given by Schyndel et al. (1994) and Wolfgang et al. (1996). More recently, Droogenbroeck et al. (2002) have proposed an entropy-based technique for LSB data embedding in images with a specific target, sometimes referred to as feature location defined by Bender et al. (1996).

3. MULTISTREAM CIPHER STEGNOGRAPHY

In spatial domain (RGB, YUV, YIQ, YCbCr, SMPTE-240M and CMY,K colour coordinate systems), least significant bit planes of natural images have a tendency to look random Droogenbroeck et al. (2002) as illustrated on Lena in Figure 3.1.

In higher bit planes neighbouring pixels are statistically very correlated. Techniques that substitute bits normally presume that values are disparate in least significant bit planes in order to conceal or embed a signal. LSB embedding permits high perceptual transparency but it is susceptible to alteration and removal. To overcome these we propose a scheme that provides superior security, integrity and capacity. In our proposed scheme we make use of a variation of the Spread Spectrum and entropy based LSB embedding techniques. First of all the signature is encrypted using an advance symmetric cipher. The cryptogram is then spread over the cover video signal using five cryptographically secure pseudorandom bit generators (CSPRBG). The CSPRBG-1 is used to spread the narrowband signal of the signature across a wideband waveform. This waveform is embedded into the cover into bit positions specified by the other four cryptographically secure pseudorandom bit generators. CSPRBG-5 selects random frames for embedment, CSPRBG-4 selects random pixels for embedment, CSPRBG-3 selects random pixel bit planes and CSPRBG-2 selects random least significant bits for embedment. In order not to compromise the overall video quality, the algorithm adaptively limits the maximum number of least significant bits for embedment by entropy estimation as proposed by Droogenbroeck et al. (2002). Based upon the image contents of any video frame this number could vary from 1 to 4. This allows larger files like video, voice and images to be sent as signatures in the host video file. The scheme uses the symmetric cipher for two purposes one for security and the second for integrity. Any single bit modification to the embedded signature is easily detectable and the signature is discarded thus providing integrity of the embedded message. Also if the message or its hash is encrypted using the sender’s private key it provides authenticity to the recipient. The proposed scheme can also be used for cascaded-encipherment where the stego-video becomes the signature to another host video thus providing multiple layers of security.
The embedding process is as shown in Figure 3.2. The steps of the scheme during the embedding phase are as follows (we assume that each frame is defined on 24 bits):

a) The message of length $n$ is first encrypted using a symmetric key algorithm using Key-0 to produce a set of encrypted bits $E_n$.

b) CSPRBG-1, CSPRBG-2, CSPRBG-3, CSPRBG-4 and CSPRBG-5 are initialised with respective seeds Key-1, Key-2, Key-3, Key-4 and Key-5.

c) Each bit $E_n$ is XORed with the CSPRBG-1 to generate a random bit ($R_n$).

d) CSPRBG-5 determines the use of a particular frame ($F_n$).

e) CSPRBG-4 determines the use of pixels ($P_n$) in each frame.

f) CSPRBG-3 determines the use of bit planes ($C_n$) of each pixel.

g) Entropy of each 8x8 block of pixels is computed on the 4 MSB. If the entropy is larger than 2 then the max number of LSB ($B_n$) is set to 4 else the entropy is calculated on the 5 MSB. If this entropy is larger than 2 then the max number of LSB is set to 3 else to 2. The use of an individual LSB out of the max number of LSB is determined by CSPRBG-2.

h) Each bit $R_n$ computed in step c) is placed at bit position determined by ($F_n$, $P_n$, $C_n$, $B_n$).

i) Steps c) to h) are repeated in nested form until the complete message is embedded and stego-video is obtained.

![Diagram](Cover Video) → Video Decoder → Frame Extraction

![Diagram](Key-5) → CSPRBG-5 → Frame Selection

![Diagram](Key-4) → CSPRBG-4 → Pixel Selection

![Diagram](Key-3) → CSPRBG-3 → Bitplane Selection

![Diagram](Key-2) → CSPRBG-2 → LSB Selection

![Diagram](Key-1) → CSPRBG-1 → Embedding

![Diagram](Key-0) → Encryption → Video Encoder

Message → Stego Video

Figure 3.2 : Embedding Process

At the reception side a similar scheme as shown in Figure 3.3, is used to extract the message from the stego-video. The following steps are performed during extraction:

a) CSPRBG-1, CSPRBG-2, CSPRBG-3, CSPRBG-4 and CSPRBG-5 are initialised with respective seeds Key-1, Key-2, Key-3, Key-4 and Key-5.

b) CSPRBG-5 determines the use of a particular frame ($F_n$).

c) CSPRBG-4 determines the use of pixels ($P_n$) in each frame.

d) CSPRBG-3 determines the use of bit planes ($C_n$) of each pixel.

e) Entropy of each 8x8 block of pixels is computed on the 4 MSB. If the entropy is larger than 2 then the max number of LSB ($B_n$) is set to 4 else the entropy is calculated on the 5 MSB. If this entropy is larger than 2 then the max number of LSB is set to 3 else to 2. The use of an individual LSB out of the max number of LSB is determined by CSPRBG-2.

f) Each bit $R_n$ is extracted from the bit position determined by ($F_n$, $P_n$, $C_n$, $B_n$).

g) $R_n$ is XORed with the CSPRBG-1 to generate the encrypted bit $E_n$.

h) Steps b) to g) are repeated in nested form till the extraction of all the encrypted bits.

i) The cryptogram created in step h) is decrypted using the same symmetric key algorithm with Key-0.
For clarification, three frames each of 2x2 pixels are shown in Figure 3.4. If frame selection is enabled i.e. CSPRBG-5 is disabled, an information embedding rate of 5.75 bits per pixel is achieved using the proposed scheme. However, if frame selection is enabled the rate drops to 3.83 bits per pixel. Thus by triggering different pseudorandom generators, variable-embedding rates can be achieved according to signature size and level of secrecy required.

Figure 3.4 : Sample Pseudorandom Streams

4. PERFORMANCE VS. CAPACITY

To investigate the performance and capacity of the Multi-Stream Cipher steganographic technique an image processing application was developed that implemented the said scheme. A 24-bit colour image of Lena was used as the host file representing a single digital video colour frame. Several tests were carried out to measure the performance and capacity of the scheme using signatures of different types (image, video, audio, text etc) and sizes (12, 24, 36, 48, 60, 72, 84, 96, 38 KB). The type of Encryption algorithms and Pseudo Random generators used in the experiments is given in Table 4.1. The signatures were hidden in the same host file using variable number of least significant bits and the test results are depicted in Figure 4.1.

Table 4.1 : Test Parameters

<table>
<thead>
<tr>
<th>Host file specifications</th>
<th>Size 768KB, Resolution 512x512 Pixels, 24 bit colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature file size</td>
<td>12, 24, 36, 48, 60, 72, 84, 96, 38 KB</td>
</tr>
<tr>
<td>Block Cipher</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CSPRBG-1</td>
<td>RSA Pseudorandom Bit Generator</td>
</tr>
<tr>
<td>CSPRBG-2</td>
<td>Blum-Blum-Shub Bit Generator</td>
</tr>
<tr>
<td>CSPRBG-3</td>
<td>Micali-Schnorr Bit Generator</td>
</tr>
<tr>
<td>CSPRBG-4</td>
<td>RC4</td>
</tr>
<tr>
<td>CSPRBG-5</td>
<td>Alternating Step Generator</td>
</tr>
</tbody>
</table>
The quality of these cover images was then verified using IQM Nill (1992) that is an objective image quality measure based on the digital image power spectrum. The measure incorporates a representation of the human visual system, a novel approach to account for directional differences in perspective for obliquely acquired scenes, and a filter developed to account for imaging system noise as specifically evidenced in the image power spectra. The image quality measure versus signal to noise ratio achieved for the test stego-images is shown in Figure 4.2. As seen in the figure, the proposed scheme achieves an Image Quality factor that is slightly lower than the 9 bits/pixel steganographic scheme. This slight loss of image quality is compensated by the multi fold increase in data security due to variable data placement in the least significant bits of the cover image. However, the steganographic SNR, the ratio of the embedded signal power to the cover image power, has been increased from 0.539 db to 0.547 db. This realization of an exceptionally high Signal to Noise ratio makes the proposed scheme most appropriate for high volume data concealment like picture-in-picture and video-in-video applications. The steganographic capacity for this image at a SNR of 0.547 db is lower bounded by 3 and upper bounded at 12 information bits per pixel based upon the local entropy calculation. However, as seen by the figure, data embedding beyond 12 bits/pixel shows a rapid degradation in the image quality.

5. STEGANALYSIS OF PROPOSED SCHEME

The presence of a pseudo-random signal embedded in the least significant bits of a colour image can be detected due to the existence of typical distributions of colour values in natural or artificial images Fridrich et al (2000). The detection mechanism is particularly efficient when bit plane values are more associated than the embedded signal. The dependability of the detection method augments with the diminishing number of unique colours in the original image. Fridrich et al (2001) proposes that messages embedded in LSB requiring less than 0.005 bits per pixel are undetectable using RS Steganalysis. This rate of data embedding may be appropriate for watermarking but is inadequate for high capacity data embedding. To maximize the bits per pixels, an entropy-based scheme that can embed up to 4 bits per pixel with minimum of 2 bits per pixel can be used Droogenbroeck et al. (2002).

The proposed scheme also makes use of entropy based LSB selection along with multiple pseudorandom generators to distribute the message as randomly as possible over arbitrarily chosen frames of the host video. The use of variable LSB in each pixel bit plane makes the scheme robust to available steganalysis methods. Also as the signature is spread over random frames it makes the scheme more detection resistant. The maximum size of the signature that can be embedded inside a specific carrier is dependent on the randomness of an image contents. If a video consists of frames that have elevated amount of randomness, then based upon the entropy, a large amount of data can be embedded into the pixels. However, if the image contents are not very random, this rate is reduced based upon the entropy estimation. As long as the embedded signal remains invisible there is no upper bound to the amount of embedded information, but the larger the amount of information the easier it is to detect the presence of an embedded signal. However, real applications require knowing in advance the number...
of bits that can be embedded in a host video file. As this number depends on the frame content as well as the pseudorandom streams, it is impossible to provide a general upper bound. The theoretical upper bound to the amount of data that can be embedded into each video frame is shown in Figure 5.1.

![Figure 5.1: Maximum possible signature data rates for uncompressed video frames (8, 16, 24 bit)](image)

Since images may display distortions from concealed information Johnson (1998a, 1998b), selecting the appropriate carrier is the key to successful information hiding. Some images may become disgustingly corrupted with even small amounts of embedded information. This “visible noise” will give away the existence of hidden information. Only after assessing many original images and stego-images as to colour composition, luminance, and pixel associations do incongruities point to characteristics that are not common in other images. Patterns become observable when evaluating a range of images used for applying steganography. Such patterns are generally the bizarre sorting of colour palettes, associations between colours in colour indexes, embellished noise etc. An approach used to recognize such patterns is to evaluate the original cover-images with the stego-images and note perceptible dissimilarities (known-cover attack Johnson 1998c). To avoid such an attack it is recommended that the original cover video may never be disclosed or be embedded with noise so as conceal its originality.

6. CONCLUSION

In this paper we have proposed a technique to embed information as randomly as possible inside the frames of digital video in spatial domain. The scheme is unique in the sense that it makes optimal use of the pixels in digital video frames by taking the local entropy into account and randomly distributes the signature in them, resulting in a remarkably high Signal to Noise ratio. In our technique, the data to be concealed is first encrypted using a symmetric cipher and then spread over the individual colour bands of each pixel of each video frame using multiple cryptographically secure pseudorandom bit generators. At the reception side, a similar algorithm extracts the embedded signal without the need of additional information. We have also analysed the performance and capacity of our proposed scheme through actual implementation. The results have shown that the scheme can effectively achieve a data-hiding rate of more than 9 bits/pixel with minimal loss of host video quality making it a suitable candidate for high volume data hiding applications.

7. REFERENCES


8. COPYRIGHT

[Asad Amir Pirzada & Raja Iqbal] © 2003. The author/s assign the We-B Centre & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the We-B Centre & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.