JPEG BASED CONDITIONAL ENTROPY CODING FOR CORRELATED STEGANOGRAPHY

Lei Zheng, Ingemar J. Cox

Department of Electronic and Electrical Engineering, University College London, United Kingdom

ABSTRACT

Correlated steganography considers the case in which the cover Work is chosen to be correlated with the covert message that is to be hidden. The advantage of this is that, at least theoretically, the number of bits needed to encode the hidden message can be considerably reduced since it is based on the conditional entropy of the message given the cover. This may be much less than the entropy of the message itself. And if the number of bits needed to embed the hidden message is significantly reduced, then it is more likely that the steganographic algorithm will be secure, i.e. undetectable. In this paper, we describe an example of correlated steganography. Specifically, we are interested in embedding a covert image into a cover image. Comparative experiments indicate that selecting a cover Work that is correlated with the covert message can reduce the number of bits needed to represent the covert image below that needed by standard JPEG compression, provided the two images are sufficiently correlated.

1. INTRODUCTION

Steganography provides a covert communication channel between two parties. The problem is typically framed as the Prisoners' Problem [1] in which two prisoners, Alice and Bob, are permitted to communicate between one another while under the surveillance of a Warden, Eve. It is usually assumed that the Warden is passive, i.e. Eve will inspect Works sent by Alice, apply a steganalytic test to determine whether the Work contains a covert message, and forward the message to Bob, if the test is negative. However, if the test is positive, Eve will not forward the message, thereby preventing any covert communication.

The goal of any steganographic algorithm is, therefore, to be undetectable. Cachin [2] defined undetectability in an information theoretic framework, stating that perfect security (undetectability) can be achieved provided the probability distribution functions (pdf) of the cover Works and the stego Works are identical. The system is considered to be ε-secure, if the Kullback-Leibler distance between the two distributions is less than ε. Various steganographic frameworks have been proposed in order to achieve undetectability in the sense of Cachin. These can be classified into three broad groups: model-based [3], statistics-preserving, such as OutGuess [4], and masking-based, such as stochastic modulation [5]. In addition, several techniques have recently been developed to minimize the embedding impact, specifically, syndrome coding [6] and wet paper codes [7]. Our approach can be considered to complementary in that our goal is to reduce the number of bits needed to encode the message. The resulting code could then be embedded using one or other of the methods above, albeit with some modifications.

Evaluation of the security of steganographic algorithms is usually performed as a function of the relative length of the embedded message, which is the ratio of the message length to the maximum message length. For example, if LSB embedding is used, then the maximum message length is the number of pixels in the cover image, but the actual message length can be much shorter. It is common knowledge that the smaller the message is, the more difficult it is to detect. For instance, it is trivial to embed an undetectable message length, say 8-bits, and guarantee undetectabilty. In fact, in this case, it is not even necessary to alter the cover Work, but just to choose a cover Work that hashes to the desired 8-bits value. Steganographic research therefore focuses on developing secure algorithms with large message length.

The fact that security is easier to achieve if the message length is shorter suggests another direction of research known as correlated steganography [8, 9]. Previous work has assumed that the cover Work is uncorrelated with the hidden message. The sole purpose of the cover Work is to hide the embedded message. In this case, the hidden message is first compressed and then encrypted prior to embedding in the cover Work. However, correlated steganography utilizes the cover Work to allow the secret message to be more efficiently encoded.

It is well-known that the minimum number of bits needed to compress a message is given by the entropy of the message. However, if the message is correlated with the cover Work, then the minimum number of bits is given by the conditional entropy. If the message and cover Work are sufficiently correlated, then the number of bits needed to represent the message may be very much less than the entropy of the message. In this case, fewer bits need to be embedded in the cover Work, and detection by steganalysis should therefore be more difficult. Interestingly, in [8], it

was shown that the information received by Bob can be very much greater than the number of embedded bits. In the limit, it achieves the entropy of the cover Work. This is because the cover Work also provides information to Bob, as it defines a probability distribution with which to very efficiently encode the hidden message. Note that while correlated steganography can aid in the design of a Cachin-secure steganographic algorithm, it is not necessarily secure in the Shannon sense. This issue is discussed in [8].

In [8], an example of correlated steganography was provided based on an algorithm originally proposed in [10]. In the next section, we describe an improved version of this algorithm for embedding an image within an image. Section 3 then provides experimental results comparing the number of bits needed to encode the hidden image using our conditional entropy coding with the number of bits needed using standard JPEG compression. Section 4 concludes with a summary and discussion.

2. JPEG BASED CONDITIONAL ENTROPY CODING

We consider the situation in which we wish to embed a hidden graylevel image within a cover image of the same or larger dimensions. Our proposed conditional entropy coding proceeds as follows:

1. Partition the cover image, $\boldsymbol{c}$, and hidden image, $\boldsymbol{m}$, into 8×8 blocks, each block is denoted by $\boldsymbol{c}_i$ and $\boldsymbol{m}_j$ respectively. The discrete cosine transform (DCT) of each block is denoted by $\boldsymbol{C}_i$ and $\boldsymbol{M}_j$ respectively.
2. The error matrix $\boldsymbol{E}_{i,j}$ between two blocks, $\boldsymbol{C}_i$ and $\boldsymbol{M}_j$, is defined as
$$\boldsymbol{E}_{i,j}(u,v)=\begin{cases}\boldsymbol{M}_j(u,v) & u,v=0\\ \boldsymbol{M}_j(u,v)-\boldsymbol{C}_i(u,v) & u,v=1,2,\cdots,7\end{cases} \quad (1)$$
where $\boldsymbol{M}_j(u,v)$ and $\boldsymbol{C}_i(u,v)$ are the DCT coefficients of the 8×8 blocks $\boldsymbol{M}_j$ and $\boldsymbol{C}_i$ respectively, and $\boldsymbol{E}_{i,j}(u,v)$ are the elements of error matrix $\boldsymbol{E}_{i,j}$.
3. For each block of the hidden image, $\boldsymbol{M}_j$, find the closest block, $\boldsymbol{C}_i$, in the cover image such that the sum of squared errors, $S_{i,j}$, between corresponding AC coefficients is a minimum.
$$S_{i,j}=\sum_{u=1}^{7}\sum_{v=1}^{7}\boldsymbol{E}_{i,j}^2(u,v) \quad (2)$$
For each given block $\boldsymbol{M}_j$ in the hidden image, we denote the index i with the minimum distance in the cover image by $B(j)$.
4. The associated error matrix $\boldsymbol{E}_{B(j),j}$ is then quantized, and the elements are arranged in the JPEG zigzag order.
5. For each block of the hidden image, the run length encoding (RLE) is used to code the quantized AC coefficients as well as the differential pulse code modulation (DPCM) is used to code the quantized DC coefficient. Both data streams are then canonically Huffman encoded.

Note that the sum of squared errors is computed only over the AC coefficients and ignores the DC coefficient of each block, which is coded separately. The DC coefficient is ignored as its magnitude is often much larger than the AC coefficients. Thus, if the DC term is incorporated into Equation (1) and (2), the sum of squared errors is dominated by the difference in the DC coefficients. Consequently, the search for similar blocks reduces to find two blocks that have approximately the same brightness, even though their AC coefficients may be very different. To avoid this, we ignore the DC coefficient in our calculation of Equation (2), which only measures the difference in AC coefficients, determining the texture and detail of each block. Thus, the two blocks that have minimum distance will be most similar in texture and detail, even though their average brightness may be very different. Although we ignore any correlation between the DC coefficients in the hidden and cover blocks, we exploit the spatial correlation within the hidden image itself to encode the DC coefficient using DPCM coding. However, it should be noted that this correlation is not the same as the correlation used for conditional entropy coding. Emphasizing this point, we only exploit the correlation of AC coefficients between the hidden and the cover images.

Quantization of the error matrix $\boldsymbol{E}_{B(j),j}$ is performed using the default luminance quantization matrix of JPEG, which is shown below:

$$\boldsymbol{Matrix}_{Quant}=\begin{bmatrix}16&11&10&16&24&40&51&61\\12&12&14&19&26&58&60&55\\14&13&16&24&40&57&69&56\\14&17&22&29&51&87&80&62\\18&22&37&56&68&109&103&77\\24&35&55&64&81&104&113&92\\49&64&78&87&103&121&120&101\\72&92&95&98&112&100&103&99\end{bmatrix} \quad (3)$$

Similarly, we use the standard codebook of canonical Huffman coding in JPEG, to code our quantized $\boldsymbol{E}_{B(j),j}$ data. This has the advantage that we do not have to embed either the quantization matrix or the Huffman table, since both can be assumed known by the embedder and the decoder. Therefore, the number of bits needed to encode the hidden image is reduced.

Thus, the output bit stream that must be embedded in the cover image consists of only two parts, the error matrix $\boldsymbol{E}_{B(j),j}$ and the block index $B(j)$. If there are total n blocks in the cover image, then each block index is represented by $\lceil log_2(n) \rceil$ bits. In this paper, we do not consider compressing these bits. However, this issue is discussed in the Section 4.

3. EXPERIMENTS

In this section, we first examine how the choice of cover image can affect the compression of the hidden image, and then investigate two extreme cases, one in which the cover

and hidden images are very similar and one in which they are identical. Obviously the latter situation has not practical purpose, but it serves to identify the limits to the performance of our algorithm.

To examine the affect of the cover image on the compression capability of our algorithm, we use the Lena image of Figure 1 with dimensions 128×128 as the hidden image. We then embed it in each of 1000 cover images with dimensions 768×512 from the Corel image database. Strictly, the Lena image we embed is a compressed version.

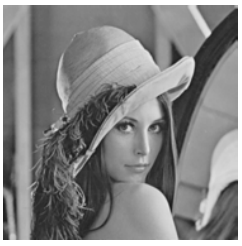

Figure 1. Lena: 128×128 pixels

If we use JPEG baseline sequential coding to compress the hidden image, Lena, it requires 1.6816 bits/pixel, and the decompressed image has a 31 dB *PSNR* compared with the original uncompressed image, where *PSNR* is defined as

$$PSNR = 10\lg\frac{255^2}{\frac{1}{m\cdot n}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{i,j}-x_{i,j}')^2} \qquad (4)$$

and $x_{i,j}$ denotes the original pixel value, and $x_{i,j}'$ denotes the decompressed pixel value.

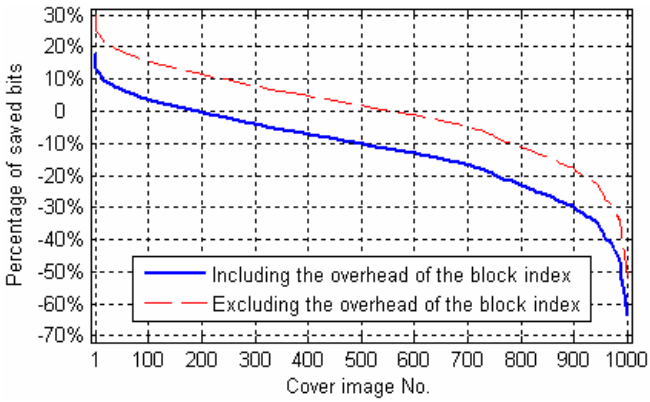

Figure 2. Percentage of saved bits compared with JPEG compression. The 1000 cover images are in descending order with respect to bits saved. Negative values indicate that more bits are needed than for JPEG compression.

Figure 2 shows the percentage of saved bits compared with using JPEG coding. The 1000 cover images are in descending order of improvement. The dashed line excludes the bits needed to encode the block index, and the solid line includes the block index. In each of the 1000 covers, the hidden image, Lena, is recovered at a *PSNR* of 31 dB, i.e. with the same distortion as for JPEG compression.

It is evident that the choice of the cover image can have a very significant impact on the compression achievable. In the best case, the cover for which is shown in Figure 3, we see an improvement of almost 30% (excluding the overhead of the block index) and 18% with the overhead. Table 1 summarizes the results for the best case.

Figure 3. Best cover image for Lena: 768×512 pixels

Our conditional entropy coding (*bits/pixel*)			JPEG
Error matrix $\boldsymbol{E}_{B(j),j}$	Block index $B(j)$	Total	(*bits/pixel*)
1.1826	0.2031	1.3857	1.6816

Table 1. Bits per pixel for the best case in which the Lena image is embedded in the cover image of Figure 3.

In contrast, in the worst case, there is no saving and the number of bits needed to compress the image is actually about 64% worse than for JPEG. Interestingly, for the Lena image, only about 200 of the 1000 cover images result in improved compression.

This experiment demonstrates that significant savings in message length can be achieved using correlated steganography, provided a sufficiently correlated image exists in the cover database. It also highlights the overhead due to the need to code the index of the most similar block.

Figure 4. Sequential image 1 256×256 pixels

Figure 5. Sequential image 2 256×256 pixels

To see just how much can be saved, we also examine the case in which the hidden image and cover image are very similar, by using two sequential images from the USC-

SIPI image database. Here, we use the image illustrated in Figure 4 as the cover and in Figure 5 as the hidden. The result is tabulated in Table 2, where we see that the bit saving over JPEG compression is 68%. In both cases, the *PSNR* of the recovered hidden image is 43 dB. Notice that the overhead in coding the block index is 38%.

Our conditional entropy coding (*bits/pixel*)			JPEG
Error matrix $\boldsymbol{E}_{B(j),j}$	Block index $B(j)$	Total	(*bits/pixel*)
0.2533	0.1563	0.4096	1.2946

Table 2. Relative coding costs in bits per pixel when the cover and hidden images are very similar.

In the limit, we can embed a hidden image in an identical copy of itself. Table 3 enumerates the results for the image of Figure 5. The *PSNR* of the recovered hidden image is also kept as 43 dB. Even though the AC coefficients of the error matrix $\boldsymbol{E}_{B(j),j}$ are all zero, we still incur a cost due to the DPCM coding of DC coefficient. In addition, the overhead of the block index remains the same. Ideally, the compression would be much less, illustrating limitations of our current algorithm.

Our conditional entropy coding (*bits/pixel*)			JPEG
Error matrix $\boldsymbol{E}_{B(j),j}$	Block index $B(j)$	Total	(*bits/pixel*)
0.1228	0.1563	0.2791	1.2946

Table 3. Relative coding costs in bits per pixel when the cover and hidden images are identical.

4. CONCLUSION

It is well-known that the fewer bits that are embedded in a cover image, the more difficult it is to detect the hidden message. To reduce the source coding of the hidden message, correlated steganography chooses a cover Work that is correlated with the hidden message. In so doing, the number of bits needed to encode the message can be considerably reduced. Doing so, does not compromise security in the Cachin sense. In fact, the goal is to improve it. However, there is information leakage in the Shannon sense. It remains unclear to what extent. This is a problem and is a possible direction for future work.

To demonstrate the feasibility of this approach, we propose a compression method based on [8, 10]. Experimental results show that for a 128×128 hidden image of Lena, the best cover image chosen from a database of 1000 possible cover images reduces the number of bits needed to code the image by about 18%. Much greater savings can be achieved if a more similar cover image is available.

There are a number of future directions for this current work. At an algorithmic level, it would be interesting to examine more efficient coding methods to reduce the overhead of encoding the block index. A preliminary investigation of the use of relative offset, rather than an absolute index, followed by Huffman encoding, looks promising.

More generally, the problem of correlated steganography can be posed as, for a covert message, $\boldsymbol{m}$, select a cover text, $\boldsymbol{c}$, that is correlated with $\boldsymbol{m}$, code $\boldsymbol{m}$ given $\boldsymbol{c}$ and embed the code in $\boldsymbol{c}$ to produce a stegotext $\boldsymbol{s}$, such that the Kullback-Leibler distance between the probability distribution functions of $\boldsymbol{c}$ and $\boldsymbol{s}$ is less than ε, and such that, at the decoder, the message, $\boldsymbol{m}$, can be recovered exactly given only the stegotext $\boldsymbol{s}$. The problem statement is similar to that of watermarking with side information and has been studied by [9]. However, to the best of the authors' knowledge, no algorithm analogous to, say quantization index modulation, is known.

5. REFERENCES

[1] G. Simmons, "The Prisoners' Problem and the Subliminal Channel," *Advances in Cryptology: Proceedings of CRYPTO '83*, pp. 51-67, 1984.

[2] C. Cachin, "An Information-theoretic Model for Steganography," *Information and Computation*, Vol. 192, pp. 41-56, 2004.

[3] P. Sallee, "Model-based Methods for Steganography and Steganalysis," *International Journal of Image and Graphics*, Vol. 5, No. 1, pp. 167-189, 2005.

[4] N. Provos, "Defending Against Statistical Steganalysis," *Proceedings of the 10th USENIX Security Symposium*, pp. 323-336, 2001.

[5] J. Fridrich, M. Goljan, "Digital Image Steganography Using Stochastic Modulation," *Proceedings of SPIE*, Vol. 5020, pp. 191-202, 2003.

[6] J. Fridrich, D. Soukal, "Matrix Embedding for Large Payloads," *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 3, pp. 390-395, 2006.

[7] J. Fridrich, M. Goljan, P. Lisoněk, and D. Soukal, "Writing on Wet Paper," *IEEE Transactions on Signal Processing*, Vol. 53, No. 10, pp. 3923-3935, 2005.

[8] I. Cox, T. Kalker, G. Pakura, and M. Scheel, "Information Transmission and Steganography," *Lecture Notes in Computer Science*, Vol. 3170, pp. 15-29, 2005.

[9] E. Yang, W. Sun, "On Information Embedding When Watermarks and Covertexts Are Correlated," *IEEE International Symposium on Information Theory*, pp. 346-350, 2006.

[10] C. Chan, L. Cheng, K. Leung, and S. Li, "Image Hiding Based on Block Difference," *8th International Conference on Control, Automation, Robotics and Vision*, pp. 968-972, 2004.

[11] G. Wallace, "The JPEG Still Picture Compression Standard," *IEEE Transactions on Consumer Electronics*, Vol. 38, No. 1, pp. 18-34, 1992.