High quality content reconstruction in images using a high capacity self-embedding algorithm

Hendrik J Kolver

July 17, 2014

Abstract

Abstract of this paper and what I wrote in it. This will give the reader a short overview of what they can expect to find in this paper.

Contents

1 Introduction

This section gives a brief description of the concepts used in this report. The reasoning behind the proposed method will also be explained in 1.5.1 and 1.5.2. This will serve to to show the applicability of the proposed method as well as the shortcomings it attempts to address.

1.1 Overview

Self recovering images (described in 1.4) poses an interesting problem. There is an inherent trade-off (described in 1.5) between the quality of the image after embedding and the quality of the image after recovery. This report proposes a method in which a high capacity embedding algorithm (described in 1.5.2) is applied to the problem of self-recovering images to attempt to increase the quality of the images (described in 1.5.1) both after embedding and after recovery.

1.2 Steganography

Steganography is the process of hiding information in such a way that it does not get detected [3]. Steganography, derived from Greek means "covered writing". This means it differs from cryptography which does not attempt to hide information but merely scrambles it so it cannot be understood. Steganography does not scramble the information but rather relies on the information to remain hidden.

1.3 Fragile Watermarking

Fragile watermarking is a variation of traditional watermarking where a watermark is embedded into an image such that subsequent alterations to the watermarked image can be detected with high probability [5]. This means that if modifications are made to the watermarked image it would be possible to detect that modifications were made as well as what parts of the image were modified. This is a necessary component in self recovering images because in order to be able to recover image data it first needs to be determined what data needs to be recovered. It thus needs to be know what data was modified. A fragile watermark is used for this purpose.

1.4 Self embedding and recovery

Self embedding is a scheme where image content is embedded into the image itself. This embedded content can then later be used to recover damaged or modified parts of the image without accessing the original image itself [2]. A self embedding and recovery scheme such as the proposed method contains a couple of high level steps. Firstly the authentic image content is embedded into the original image along with a fragile watermark. This watermark will help determine later on which parts of the image was modified if any (see 1.3). When the authentic image needs to be recovered, after modification, the fragile watermark is used to determine which content was modified. An attempt is then made to extract the original content for the areas that were modified from the modified image. If this process is successful the user is left with a high quality reconstruction of the original image.

1.5 Quality Trade-off

There is an inherent quality trade-off present within self embedding schemes. The trade-off exists between the image after embedding and the image after recovery. If an embedding algorith such as LSB(Least significan bit) embedding is used (as in 2.1.1) the actual bit values of the original image are overwritten. Naturally the more bit values are overwritten the more noise is introduced into the image. This effectively reduces the quality of the image after embedding.

The solution to this would be to simply embed a small amount of information into the image to

keep the noise low. However this presents another problem. The quality of the image after recovery is dependent on the amount of authentic image data embedded into the image.

To achieve maximum quality after embedding the embedded information must be as little as possible. To achieve maximum quality after recover the embedded information must be as large as possible to be as close as possible to the original image. There exists then a trade-off between the two.

1.5.1 Increasing quality with capacity

It might be possible to increase the quality of the image after recovery while still keeping the quality after embedding high. It is proposed that applying an embedding algorithm designed for high capacity while retaining quality (as discussed in 1.5.2) to the problem of self embedding could possibly increase the quality of the image after embedding as well as after recovery. This is because such an algorithm should provide higher embedding capacity while producing less noise in the image.

1.5.2 High capacity embedding algorithms

The proposed method in this paper attempts to apply the algorithm for BPCS Steganography [1] to the problem of self recovering images, specifically to increase overall quality.

The goal of the BPCS algorithm is to embed as much data as possible into a cover image without detection [1]. This refers to detection by human perception as well as statistical analysis although the latter is not the focus of this paper. The BPCS algorithm uses an adaptive scheme to classify blocks that are suitable for embedding (similar to 2.1.3). BPCS steg differs however in the fact that the blocks can be conjugated in a checker board pattern to increase complexity and decrease detectability if needs be.

The BPCS algorithm can achieve a very high capacity while still remaining undetectable through human perception. This makes the BPCS algorithm a possible good choice to increase the capacity of a self recovering image scheme and possible increase the quality through this process.

2 Current self embedding and recovery schemes and algorithms

This section compares current Content reconstruction algorithms using self embedding. This serves to give an overview of what is currently available and to possibly highlight shortcomings of the current algorithms. This would be useful to determine if the proposed method does indeed improve on existing methods. It would also help highlight strengths and shortcomings in the proposed method. The methods analyzed were chosen because they all provide good quality cover and reconstructed images. They also each offer an unique approach or aspect to the image recovery problem and would thus provide a good idea of the different approaches that have already been tested.

2.1 Overview

2.1.1 Erasure channel model utilizing the remaining authentic content

The method proposed in [4] uses an erasure channel as a model for the content reconstruction problem. The method uses LSB embedding to embed the reference data into the image itself. The method also uses a global spreading technique to spread the reference data across the image. They

also propose that by using the remaining authentic content in the image it is possible to have a high tamper rate while at the same time achieving good quality images before and after recovery.

The method proposed in [4] achieves good quality cover images with a PSNR >35dB. The method also achieves an image recovery quality of 35dB <PSNR >40dB and 40dB <PSNR with taper rates of 50% and 33% respectively. The method does not let the restoration quality of the image deteriorate much if the tampering rate is increased up to a value of 50%. They do however note that they can only achieve minimal reconstruction performance increases by decreasing the amount of information in the reconstruction reference. By using only 50% of the available capacity the maximal tampering rate increases form 50% to 59%.

This method [4] is thus quite robust since 50% of the image may be tampered with before recovery starts to deteriorate. The security for this method is also very good since the quality of the cover image is not very susceptible to visual checks. The authors did not do any statistical analysis on the image. The embedding capacity of this method is also acceptable, but because the method uses some of the authentic image data to aid in the recovery the quality of the image, before and after recovery, is still very good even without a very high embedding capacity.

2.1.2 Method using difference expansion

[9] Proposed a method that uses difference expansion and generalized LSB embedding. Difference expansion works by exploiting the high redundancy that are present in images. With difference expansion the payload is embedded in the difference of pixel values. For a pair of pixel values (x,y). [7] It should however be noted that image quality reduces rapidly as the payload size is increased when using difference expansion. The method uses these two techniques in combination to achieve a high embedding capacity while keeping distortion relatively low. The method achieves a PSNR >35dB after embedding. The method achieves an embedding capacity of 1.78bpp when using up to the 4th LSB on a 512x512 8bit gray-scale version of the Lena image.

The method's [9] restoration quality is acceptable at roughly 50%. The difference expansion this method uses provides extra space for embedding. The authors did thus not implement compression on the image data because of the extra space the difference expansion provides. The embedding capacity of this method could thus be further improved by compressing the embedded data. This could possibly lead to better quality than what their experimental results achieved at the expense of complexity. Difference expansion thus seems a good solution to increase the embedding capacity while still keeping the distortion low.

The authors do not mention the image tamper rate that this method [9] allows.

2.1.3 Dynamic block allocation for self embedding

(Qian et al) [6] proposes a method for fragile watermarking with good restoration capabilities using self embedding. The proposed method differs from the other methods mention in 2.1.1 and 2.1.2 due to the fact that the proposed method does not embed the information into all blocks uniformly. The proposed method classifies different blocks of the image according to the block smoothness. The less smooth the block is the more information will be embedded into it. The authors argue that the current methods that use a fixed embedding size for each block are inadequate since less information should be embedded into the very smooth blocks and more should be embedded into

the rough blocks [6].

The advantage of using this dynamic scheme is that there would be less visual distortion to the cover image. This is because if the specific block is already very rough (very busy visually) the human eye would not notice small changes. If however the specific block is very smooth (very uniform visually) the human eye is more likely to notice small changes. The proposed method thus creates less distortion in the cover image than fixed size methods while still retaining good restoration quality [6].

The method proposed by (Qian et al) [6] uses the 3 LSB bit planes to embed the needed information in. The method achieves good results in experimentation with a cover image PSNR >37dB as well as a reconstructed image PSNR = 35dB. The method also allows for a tamper rate <35%. The authors do not analyze the security of the algorithm.

2.2 Comparison

Each of the methods described in 2.1.3, 2.1.1 and 2.1.2 provide good quality cover images as well as good quality reconstructed images. There are however important differences. The method described in 2.1.1 offers a very good tamper rate of 50% compared to the method described in 2.1.3 which has a tamper rate of 35%. This means that a larger of the cove image can be tampered with while still being able to restore the image with good quality.

The method described in 2.1.2 achieves a cover image with a PSNR >35dB, the method described in 2.1.1 achieves similar results, however the method described in 2.1.3 achieves a cover image PSNR >37dB. This means that the method described in 2.1.3 would have less noise in the cover images after embedding and would thus have better overall quality of the cover images.

At almost equal tamper rates of around 33%-35% the method described in 2.1.1 achieves a restoration PSNR >40dB whereas the method described in 2.1.3 only achieves a restoration PSNR = 35dB. The method described in 2.1.2 only achieves a restoration quality of about 50% the original image. This means that the method described in 2.1.1 would generally produce better quality restored images than the methods described in 2.1.3 and 2.1.2.

This means that the method described in 2.1.1 provides the best tamper rate and the best restored image quality, and the method described in 2.1.3 provides the best cover image quality. The method described in 2.1.2 provides decent quality of the cover image as well as the restored image.

All three methods thus provide good results and would serve as a good benchmark for comparing the method described later in this paper.

3 Implementation

3.1 Embedding

3.1.1 BPCS Steg

In order to be able to recover the image after it has been tampered with the image needs to be embedded into itself. For this embedding the proposed method used BPCS Steganography [1].

This method works with the following steps:

1. Get the binary representation of the image
2. Convert the binary representation into Gray code
3. Divide the image into bit planes
4. Divide the bit planes into 8x8 blocks
5. Calculate the complexity for each block //TODO find reference for how this is done
6. Divide the message to be embedded into similar binary 8x8 blocks
7. Calculate the complexity for each message block and conjugate if not complex enough
8. for each image block that is complex enough, replace that block with the next message block
9. Convert the blocks back to binary representation
10. reconstruct the image from the processed blocks

The proposed method works with colour images which means that for each pixel there is a red, green and blue value. This means that each block effectively store 3 bits for each pixel.

BPCS Steg has an inherent property that if any part of the image is modified the embedded message will be lost. This would obviously be a problem for the proposed method since the image will definitely be modified.

As a solution to this problem each block used for embedding is treated as a separate embedding entity. There is thus no overlap between two different blocks used for embedding. With the compression method used (3.1.1) this means that effectively 7 pixels are embedded in each embedding block. Along with these 7 pixels the location of the first pixel is also embedded using two integers. This allows the extractor to be able to identify where all the extracted pixels belong in the image even if the image has been modified. This serves to give random access to the embedded content which is an essential property of self embedding as defined by (Korus et al. [4])

Total space available for embedding per block = (8*8)*3 = 64*3 = 192
Total embedded bits = (7*24) + (2*9) = 186

This means that there is an excess of 6 bits per block that are not used for embedding. This is effectively means there are 6 bits of embedding space being wasted with each block. This is caused by the need to be able to identify blocks even after the image has been modified.

Image Compression The image that is embedded into the cover image cannot be embedded with perfect quality due to space restrictions caused by the embedding algorithm. Compression however is not the focus of this study. The embedded image is thus just a resized version of the original image. A higher quality reconstruction could be achieved if a better compression algorithm is used.

Block Spread //TODO
It is very important how the embedded content is spread across the image because this affects the tamper rate
//put reference here
And explain further

3.1.2 Fragile Watermark

In order to be able to detect which parts of the image have been tampered with a fragile watermark can be used.

An initial attempt was made to apply the method proposed in [8]. This method is a reversible fragile watermark which means that the watermark can be removed to restore the original content bit by bit before watermarking if the image was found to be authentic.

The method needed to be adapted to authenticate the image on a block level, the image is divided into 8x8 blocks. The method requires compression of bit streams in order to embed the watermark and to be able to extract the watermark again. The bit streams are rather small in the proposed method because they are only applicable to a specific 8x8 pixel block. This results in the fact that there is not always enough redundancy to be able to compress the bit streams enough for embedding.

Another problem with this method was the large amount of noise that this method of watermarking introduces into the cover image since it also uses difference expansion as mentioned in [7].

The fragile watermark used in the proposed method embeds a calculated hash into the image that is used to authenticate the content when the image is processed on the receiving end.

For each of the 8x8 pixel blocks in the image a hash is calculated by combining the binary of each of the 7 Most significant bit layers of that block. This binary stream is then used as the input to the SHA-256 hash function the output is a 256 bit hash string for that image block. This hash string is then truncated to a length of 185 bits. This is done to enable the conjugation map that was generated when embedding the image content (3.1.1) to be stored at the end of the stream.

//TODO - Find reference for truncation of hash security

The conjugation map is appended to the truncated hash string to create a binary string of 192 bits. These 192 bits are finally embedded into the least significant bit plane of that specific block effectively replacing all the bits in that bit plane with the generated bit stream.

3.2 Extraction and Restoration

3.2.1 Image authentication

The first step for the image extraction and restoration process is to determine which, if any, parts of the image has been tampered with. This is accomplished by first completing steps 1-4 of the BPCS steg algorithm (3.1.1). for each block (block refers here to 8x8 pixel blocks, thus a block here contains all 8 bit planes) the authentication hash string is calculated as described in 3.1.2. The embedded hash is then extracted from the Least significant bit plane of that block. The extracted hash is then compared with the calculated hash and if they match the block is authentic.

For each authentic block the 7 most significant bit planes have their complexity calculated. If a bit plane block is found to be complex enough it is assumed that there is image information embedded into it. The embedded conjugation map is extracted at this point and if it is found that any of the complex enough bit planes were conjugated the conjugation algorithm is applied again to reverse the conjugation.

//TODO Explain the conjugation in more detail

The embedded image content is extracted at this point from the processed bit planes and the embedded image is reconstructed. The reconstructed image is then also split into pixel blocks. The original pixel blocks now get iterated and each block that was found not to be authentic is replaced by the corresponding reconstructed pixel block.

This process restores the tampered areas of the image if their matching pixel blocks could be extracted from the image. That is if the embedded blocks were not destroyed in the image modification. Obviously if too large a part of the image has been modified it would not be possible to accurately reconstruct the image because too much of the embedded image content would be lost.

References

[1] Steve Beaullieu, Jon Crissey, and Ian Smith. Bpcs steganography. *University of Texas at San Antonio*.

[2] Jiri Fridrich and Miroslav Goljan. Images with self-correcting capabilities. In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, volume 3, pages 792–796. IEEE, 1999.

[3] Neil F Johnson and Sushil Jajodia. Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, 1998.

[4] Pawel Korus and Andrzej Dziech. Efficient method for content reconstruction with self-embedding. *Image Processing, IEEE Transactions on*, 22(3):1134–1147, 2013.

[5] Eugene T Lin and Edward J Delp. A review of fragile image watermarks. In *Proceedings of the Multimedia and Security Workshop (ACM Multimedia'99) Multimedia Contents*, pages 25–29. Citeseer, 1999.

[6] Zhenxing Qian, Guorui Feng, Xinpeng Zhang, and Shuozhong Wang. Image self-embedding with high-quality restoration capability. *Digital Signal Processing*, 21(2):278–286, 2011.

[7] Jun Tian. Reversible watermarking by difference expansion. In *Proceedings of workshop on multimedia and security*, pages 19–22, 2002.

[8] Jun Tian. Wavelet-based reversible watermarking for authentication. In *Electronic Imaging 2002*, pages 679–690. International Society for Optics and Photonics, 2002.

[9] Jun Tian. High capacity reversible data embedding and content authentication. In *Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on*, volume 3, pages III–517. IEEE, 2003.