A Review on Uniform Embedding For Efficient Jpeg Steganography

Aasemuddin Quazi
PG Scholar
Department of CSE
Government College of Engg.
Aurangabad

A.K. Gulve
Associate Professor
Department of MCA
Government College of Engg.
Aurangabad

ABSTRACT

Steganography is the art and science of concealed communication with an aim to hide the secret messages in the cover medium. The concept of minimal distortion embedding has been accepted in development of the steganographic system, where a well-designed distortion function plays an important role. Majority of the steganographic methods for real-time digital media embed message communication by minimizing a suitably developed distortion function. This can be achieved by syndrome codes which give near-best rate distortion function. Here the Uniform Embedding Distortion function will be used along with the Syndrome Trellis Coding. Thus, statistical detectability will be reduced thereby improving the security.

Keywords

Steganography, minimal distortion embedding, JPEG steganography, syndrome trellis codes, uniform embedding.

1. INTRODUCTION

Steganography is the art and science of concealed communication where the sender hides the secret message in an original image to create a stego image. To conceal the presence of connection, the stego image has to be statistically undetectable from the original image. Therefore, the two main goals of undetectability and concealed payload must be dealt very carefully while developing a steganographic scheme. Generally the cover medium is a graphic file because of their universal presence in the digital world. In a more generalized way, it can be said that steganography is a two-step process. In the first step, an analysis of the cover image is done to find the insignificant bits. It is expected that modifying these bits will not cause any observable changes in the cover medium. In the second step, these bits are replaced by message bits to create the stego image. Generally these insignificant bits are the LSB's of the image. In JPEG images, modifying the LSB creates imperceptible distortions of the original image. Here the intention is to reduce these distortions and also enhance the undetectability and thereby improving the security.

JPEG is the most commonly used format for digital communication and due to this the field of JPEG steganography is being researched on an extensive basis. The Joint Photographic Experts Group (JPEG) file format stores image data in compressed form as quantized frequency coefficients [1]. The compressing steps performed by the JPEG compressor starts by cutting the uncompressed bitmap image into parts of 8 x 8 pixels [1]. The 8 x 8 brightness values are transformed into 8 x 8 frequency coefficients by using Discrete Cosine Transform (DCT) [1]. After DCT, quantization rounds up the frequency coefficients to integers in the range of -2048 to 2047. Analysis of a discrete distribution of coefficients frequency of occurrence shows two characteristics viz. I) The coefficients degree of occurrence decreases with increasing absolute value & II) The decrease of the coefficient's frequency of occurrence decreases with the increasing absolute value, that is difference between two bars of the histogram in the middle is larger than on the margin [1].

A practical method for minimising the additive distortion in JPEG steganography is to be studied. There are two main paths for designing a steganographic scheme, either design a steganographic system that preserves the cover model or design a steganographic scheme that minimise the embedding distortion. Here the use of Syndrome trellis codes (STC) is also made which can directly improve the security of the steganographic schemes. It allows them to transmit significant payloads with same embedding distortion or it can also decrease the distortion for payload.

There has been a development of lot of methods for JPEG steganography over a last few years maybe a decade, such as F5 [1], nsF5 [2], MME [3], and there are also some which have recently emerged. All of these schemes have concentrated on one concept, minimal distortion embedding strategy, which consists of a good distortion function and a well-known coding unit. In F5, the impact of embedding is treated equally for every coefficient. Due to this, minimisation of the total distortion for the respective payload corresponds to the attempt made to minimise the number or co-efficient modified or maximise the efficiency of embedding, which means the number of message bits embedded per embedding change. The security of F5 was enhanced by increasing the embedding efficiency by using matrix encoding, which can be seen as a special case of minimal distortion embedding scheme where embedding cost is same for every coefficient [1]. In [2], the wet paper code (WPC) is used nsF5, which is an improvement to F5, which deals with the shrinkage problem of F5, showing good results in coding efficiency as compared to Hamming codes used in F5. In MME for JPEG steganography the benefit of side information of uncompressed image is taken to create the distortion function, in addition to this only the coefficients with less distortion are taken for modification and more modification of coefficients can be done in comparison with matrix coding. In [4], an efficient JPEG steganographic scheme called BCHopt is proposed which is based on optimization and swift BCH syndrome coding. When compared with MME, BCHopt deals with both the rounding error and the quantization step of a creation of the distortion function, thereby providing improvement in security against steganalysis.

In [5], the use of Syndrome Trellis Coding (STC) is shown as a practical method for implementing minimal distortion embedding scheme. They have described that in accordance with the additive distortion model can reach good asymptotic bounds of embedding efficiency. With the advent of this coding method, it has become clear that further increase in secure payload for steganography can be obtained by carefully designing the distortion function instead of improving the coding scheme.

The problem of embedding needs to be understood while minimizing the distortion function. By using some numerical quantities and some performance bounds the problem can be better understood. Here it is assumed that the sender gets the payload as a pseudo-random bit stream by compressing or encrypting the original message. Here the process starts out by associating each cover image x with a pair $\{y, \pi\}$, where y is the set of stego images into which x can be modified and π is the probability distribution [5]. The problem of embedding fixed size message along with minimizing the distortion is a commonplace in steganography. If the distortion function is content driven, it is up to the choice of the sender to maximize the payload and also having a constraint on the total distortion. This correlates with a more instinctive use of steganography since images having varying levels of noise and texture which can take varying amounts of concealed payload and hence the distortion should be fixed instead of payload.

This problem of minimizing the embedding impact is described by Crandall [6] in his essay on steganography posted in the year 1998. He described that when encoder embeds at most one bit per pixel, the total sum should be maximized by making use of the embedding impact defined for each pixel. Conceptually, the encoder examines an area of the image and weights each of the options that allow it to embed the desired bits in that area & it scores each option for how conspicuous it is and chooses the option with the best score [5].

In [7], Filler and Fridrich proposed a model for the embedding cost along with the specific coefficients and considering both the neighbourhood and coefficient. By using STC they improved their cost model. Results showed that their distortion model can make the payload better in DCT domain. However according to [8], the distortion model deteriorated when the distortion is optimised and it even becomes less secure than the nsF5.

Recently, Holub and Fridrich proposed a universal distortion design called UNIWARD [9], in which the distortion functions for spatial (S-UNI), JPEG (J-UNI) and side-informed JPEG (SI-UNI) domain are derived from the wavelet domain. Contrary to the regular JPEG steganographic methods where the embedding of the secret message is done only into non-zero AC coefficients, the UNIWARD uses each and every coefficient as cover elements and thereby achieving the best security performance.

With the development of JPEG steganography, considerable progress has also been made in JPEG steganalysis. In [11], Kodovský and Fridrich suggested using a rich model with a large feature set of up to 22,510-D for steganalysis. By using the ensemble classifier [11], the rich model based steganalysis can detect most existing JPEG steganographic algorithms with a high accuracy. Thereby, the secure payload of JPEG steganography is degraded considerably, which gives rise to new challenges in JPEG steganography. Hence, it can be said that there is an increasing need for developing more secure JPEG steganographic algorithms.

In a more broad sense, it can be said that JPEG steganography involves two main features viz. a good steganographic scheme and a good distortion function. Here the target is on the development of a good distortion function with minimized statistical detectability.

2. RELATED WORK

2.1 Uniform embedding scheme

In Steganography, the sender uses a legitimate media, generally a JPEG image to conceal the secret message and communicate with the receiver. Thus, it becomes very tough to differentiate the stego image from the cover one, thus a concealed transmission of messages can be achieved. Here the message is generally embedded in the cover media by slightly modifying the elements of the cover, generally the LSB of the pixel and DCT coefficients that are quantized. In [5], the problem of minimizing the embedding impact for single-letter distortion is efficiently formulated. Let the binary vector $x_b = [x_{b1}, x_{b2}, \ldots, x_{bn}]$, $y_b = [y_{b1}, y_{b2}, \ldots, y_{bn}] \in \{0, 1\}^n$ and $m = [m_1, m_2, \ldots, m_k] \in \{0, 1\}^k$ be the LSB vector of the cover x, LSB vector of the stego y and message [5]. The additive distortion function can be seen as,

$$D(x\ ,y) \quad = \sum_{i=1}^{n} \rho i(x, yi)$$

where $\rho_I(x, y_i)$ denotes the cost of changing the i^{th} cover element from x_i to y_i. Along with the use of syndrome coding the distortion can be expressed as,

$$Emb(\mathrm{x, m}) = \arg \min \mathrm{D(x, y)}$$

$$\mathrm{Hy_b = m},$$

Where H is the parity check matrix of code C and the corresponding coset to syndrome m is C.

For the minimal distortion embedding the coding methods that are available includes hamming codes, BCH codes and also the syndrome codes. The evaluation of the performance of the coding methods for steganography can be done using the metric of coding loss which is defined as the relative decrease in payload due to practical coding,

$$L(D_e) = \frac{m_{max} - m}{m_{max}}$$

where m is the payload embedded by a given algorithm and m_{max} is the maximal payload embeddable with a distortion not exceeding D_e [12]. According to experiments conducted the syndrome trellis codes have attained a low coding loss with l = 7% - 14% according to the set parameters and this result will be very useful for the steganographic scheme.

For the distortion function, an attempt is made to design a universal one for making minimum artifacts of first and second order statistics rather than training it on a specified feature set.

For detecting the JPEG steganography, the statistics of quantized DCT coefficients are used to develop feature set for steganalysers [10]. For steganalysis, generally histogram and block co-occurrence matrix of DCT coefficients are used.

After the payload is embedded in the JPEG image, the DCT coefficient statistics might be modified up to some point, which might become very useful for steganalysis. The effects of data embedding on the statistical data of DCT coefficients are well illustrated with nsF5 [3]. To get more knowledge about the artifacts analysis can be done about how nsF5 works. For a particular payload nsF5 embedding simulator starts by calculating the theoretical bound of the embedding and fetches the number of coefficients to be modified. Then n non-zero AC coefficients are selected at random and their absolute value is decreased by 1. Here the use of *p(x)* and $p_{nz}(x)$ is done for the for the empirical probability density function (PDF) of the AC and non-zero AC coefficients. There is a requirement of modifications to be done of $n.p_{nz}(x)$ AC coefficients at bin x. Hence the changes caused by the message embedding in PDF can be given as

$$\Delta p(x) = \begin{cases} n\,.[\,p_{sel}(x-1) + \,p_{se1}(x+1)]/N, & if x = 0 \\ n\,.[\,p_{sel}\big(x + sgn(x)\big) + \,p_{sel}(x)]/N\,, & if x \neq 0 \end{cases}$$

Where, $p_{sel}(x) = p_{nz}(x)$ is the probability that coefficient x is selected and N denotes the total number of block DCT coefficients [12].

Taking into consideration of the fact that the DCT coefficients are on an approximate the Laplacian distributed and the random nature of selection of nsF5, the coefficients to be modified are probably those with small magnitudes. Thus, majority of the changes in the coefficient are due to the embedding scheme are around bin zero. As observed by the author in [12], majority of the coefficients that are required to be changed are present within the bins of absolute value 2. According to [3], the changes of statistics in bin 0 and ±1 arising from random embedding are significantly larger than the ones in other bins.

By taking advantage of the specified distribution artifacts of DCT coefficients with small magnitudes, even with the given threshold, most steganalysers can detect JPEG steganography with high accuracy. Here the number of modified coefficients can be reduced if a much efficient coding scheme is adopted, the distribution of the modified coefficients, yet, they would remain same after embedding. To prevent the abrupt change of statistics in small DCT coefficients, uniform embedding (UE) is preferable rather than the random embedding scheme.

$$p_{sel}(x + sgn(x)) \cong p_{sel}(x), \quad x \in \{-1024,\ldots,-1,1,\ldots., 1024\}$$

The Uniform embedding strategy spreads the embedding modifications to coefficients of all relative magnitudes so that it can minimize the statistical changes in every bin which can be shown as,

$$\Delta p\big(x + sgn(x)\big) \cong \Delta p(x), x \in \{-1024,..,-1,1,..,1024\}$$

Let M be the given message and let ΔM be the modification, *UN* and *RN* be the bin numbers involved in uniform and random embedding, respectively. The “spread magnitude” nature of uniform embedding makes *UN* >> *RN*, therefore the average modification per bin (*ΔM* / *UN*) for uniform embedding is much less than one (*ΔM* / *RN*) for random embedding. This method attempts to reduce the change of both first order and higher order statistics.

Generally, the uniform embedding strategy can be implemented using STC [5]. To embed the given message, STC gives us multiple code words, from which, a distortion function is then used to choose the one having the lowest distortion. To achieve the uniform embedding, the distortion function, to be used, should be designed such that the coefficients having different magnitudes are selected with a same priority. Such a function can be termed as Uniform Embedding Distortion Function (UED).

It can be seen that the DCT coefficients having considerable magnitudes are more likely to be modified extensively than the previous approaches, such as nsF5. Currently, the steganalysis analysers for JPEG generally make use of natural image model in terms of first- and second-order statistics of quantized DCT coefficients. When the distribution of DCT coefficients is accurately characterised by the image model, then any slight modification in the cover image would be reliably detected. But to the good fortune the distribution of DCT coefficients in images largely depends on the content and it is different for different images. In other words, the statistics of natural images indeed exhibit, to some extent, deviation away from their models of any kinds, which are what the potentials of natural images left for steganography [12].

2.2 Minimizing Additive Distortion in Steganography using Syndrome-Trellis Codes

Here a full practical method is given for minimising the additive distortion by using general i.e. non-binary embedding operation. Each possible value of every stego item can be designated a scalar value which can express the distortion caused by the embedding done by changing the cover element with this value. Here an assumption is made by the author [5] that the total distortion is the sum of per-element distortions. The payload limited sender and distortion limited sender are both considered. Payload limited sender performs the embedding of fixed average payload of n bits along with the minimization of the average distortion. Distortion limited sender performs the maximisation of average payload along with the introduction of fixed average distortion.

During the embedding, the non-binary cases are changed into a number of binary cases by changing the bits in the cover. The binary case is handled by the Syndrome trellis codes along with the Viterbi algorithm.

2.3 F5 Steganography

The F5 algorithm provides large steganographic capability and it can also deal very efficiently with visual and statistical attacks. F5 algorithm uses matrix encoding technique to increase the performance of embedding. It is known that the images provide limited steganographic capabilities, also many a times embedding work do not require the full capacity of the image. Thus, it can be said that some part might be left unused.

Some of the prominent steganographic algorithms attempt to scatter the message over the entire cover element. This might cause them to have a bad time complexity. This may be the case when the algorithm tries to use up the capacity of the image completely. The task of straddling can be made easy if the exact capacity of the carrier element is known. A permutation is used in the straddling process of F5 to mix all the coefficients, and then the embedding of the permuted sequence is done. There is no change in the number of coefficients and also their values due, to the shrinkage. Here a key is responsible for the permutation which is derived from a password. The original sequence of the modified coefficients is sent to the Huffman coder in F5 steganography. If the correct key is provided to the receiver he can once again repeat the permutation. The permutation has linear time complexity *O(n)* [1].

Here the technique, that was used to improve the efficiency of embedding, was matrix encoding. F5 algorithm is the first algorithm to make use of matrix encoding technique. If there is the lot of unused capacity of stego element then the matrix encoding can reduce the number of changes that are required to be done. The author [5] makes an assumption that there is a uniformly distributed secret message and uniformly distributed values present at some positions which are required to be changed. Also, changes are done in one-half only and the other half is left unchanged.

3. PROPOSED WORK

In the proposed model, hiding the details in the image is done mainly using the UED and the security of the steganographic image is improved by using the STC technique. In the existing systems, some drawbacks are present, if the data is hidden in the JPEG images it can be easily cracked and the data can be viewed easily by unknown persons. In the proposed system, the focus is on the distortion function along with other techniques to improve the efficiency, as well as the security of the system. According to the concept of the spread spectrum communication the distortion function, uniformly spreads the embedding changes to DCT coefficients of each and very magnitude.

The first step is to merge the secret data into the image to form the stego image. After adding the secret data, the cover image will change into the stego image. Then the SHA 256 hash function will be used to generate a fixed-length hash value for the stego image. The number of rows and columns for stego image are set and based on these numbers the splitting of the image is done. The splitting is done based on image rows and columns. Now UED algorithm is used to minimize the distortion and the STC technique is used to improve the security. To reduce the distortion, the calculation of the distortion is required to be done. After this the distortion is reduced using the UED. The main advantage in doing so is that it will increase the quality of the stego image and it will also give more security to data. The scheme is expected to give good performance in terms of secure embedding capacity against steganalysis. Fig. 1 illustrates the proposed framework for the steganography.

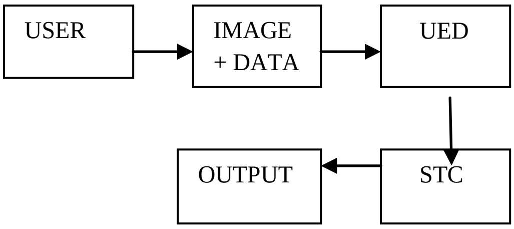

Fig. 1. Proposed Steganographic scheme

3.1 Syndrome-trellis codes

The motive behind using STC is not new from the information theoretic perspective, as the STCs are convolutional codes that can be represented in a dual domain. As STCs can be used for solving both embedding problems by providing a small coding loss even over a considerable range of distortion profiles even with wet pixels, so they have become interesting phenomena in field of steganography and it also provides practical implementation. The same code can be used for all thus making the embedding algorithm universal. STCs provide general and up to date solutions for both embedding problems in steganography. The knowledge of convolutional codes which are used in data hiding applications is a prerequisite. An effort will be made to develop an efficient coding scheme for arbitrary payload. In steganography, the relative payload is required to decrease with the increasing payload so that it can maintain the similar level of security.

Since Shannon [14], described the problem of source coding in 1959, convolutional codes were the first practically used codes for the problem. This is because the gap between the bound on the expected per pixel distortion and the distortion obtained using the optimal encoding algorithm (the Viterbi algorithm) decreases exponentially with the constraint length of the code [5]. Convolutional codes can be described by using shift registers that can generate from the set of information bits. Convolutional codes in syndrome trellis description are usually used in the problems that are dual to this problem. The disadvantage of convolutional codes is that when they are implemented by using shift register they do not fulfil the requirement of small payload which is required for steganography. In the dual domain, a code of length n is represented by a parity-check matrix instead of a generator matrix as is more common for convolutional codes [5].

The working of the syndrome trellis codes starts out by assigning every cover element an embedding distortion and then embeds the payload with as little distortion as may be possible. It gives the embedding and extraction mapping as,

Emb: $\{0, 1\}^n$ x $\{0, 1\}^k \rightarrow \{0, 1\}^n$

Ext: $\{0, 1\}^n \rightarrow \{0, 1\}^k$, satisfying

Emb(x, m) = y ,

Ext(y) = m

¥$x, y \epsilon \{0, 1\}^n$, ¥$m \epsilon \{0, 1\}^k$

where, x is the cover image and *m* is the message sequence and *y* is the stego image. The described methodology can adjust k bit message in an n element cover, along with keeping the distortion as little as possible. In Syndrome trellis coding, extraction mapping and embedding is accomplished using a binary linear code *C* and length *n* and dimension n- k. Assuming H as the parity check matrix for the above equations, the extraction mapping becomes,

Ext(y) = H*y* = *m*

Assuming C(*m*) = {$z \epsilon \{0, 1\}^n \mid Hz = m$} is the cost relating to the message sequence. The STC method can find the best z closest to x from the cost *C*(*m*) and takes it and takes it as output *y*,

$$Y = Emb(x, m) = arg_{y \epsilon C(m)}^{min}(D(x, y))$$

It should be taken into account that STC can enhance the efficiency of embedding very comprehensively at lower embedding rates.

4. CONCLUSION

The minimal distortion embedding scheme provides us with an approach that can be used and implemented practically for obtaining high embedding efficiency for JPEG steganography. Here, the JPEG steganographic scheme can be made efficient by combining the Syndrome trellis codes (STC) with Uniform embedding (UED). The uniform embedding matches with the spread spectrum communication. It can be said that if there isn't any use made of the DC and zero AC coefficients properly it might cause extra block artifacts in stego image and also deteriorate the performance of embedding. Due to this reason most of the JPEG steganographic methods use non-zero AC coefficients as the cover elements to make the embedding more efficient. The scheme studied above cannot tackle all these issues and it would be a good approach to evaluate the embedding costs of all the DCT coefficients based on the DCT domain of JPEG steganographic systems.

5. REFERENCES

[1] A. Westfeld, “F5—A steganographic algorithm,” in Proc. 4th Inf. Hiding Conf., vol. 2137. 2001, pp. 289–302.

[2] J. Fridrich, T. Pevný, and J. Kodovský, “Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities,” in Proc. 9th ACM Workshop Multimedia Security, Dallas, TX, USA, Sep. 2007, pp. 3–14.

[3] Y. Kim, Z. Duric, and D. Richards, “Modified matrix encoding technique for minimal distortion steganography,” in Proc. 8th Inf. Hiding Conf., vol. 4437. Jul. 2006, pp. 314–327

[4] V. Sachnev, H. J. Kim, and R. Zhang, “Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding,” in Proc. 11th ACM Workshop Multimedia Security, Sep. 2009, pp. 131–140.

[5] T. Filler, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using syndrome-trellis codes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[6] R. Crandall, “Some notes on steganography,” in Steganography Mailing List [Online]. Available: http://os.inf.tu-dresden.de/ westfeld/ Crandall.pdf 1998.

[7] T. Filler and J. Fridrich, “Design of adaptive steganographic schemes for digital images,” Proc. SPIE, vol. 7880, p. 78800F, Jan. 2011.

[8] J. Kodovský, J. Fridrich, and V. Holub, “On dangers of overtraining steganography to incomplete cover model,” in Proc. 13th ACM Workshop Multimedia Security, New York, NY, USA, Sep. 2011, pp. 69–76.

[9] V. Holub and J. Fridrich, “Digital image steganography using universal distortion,” in Proc. 1st ACM Workshop Inf. Hiding Multimedia Security, 2013, pp. 59–68.

[10] J. Kodovský and J. Fridrich, “Steganalysis of JPEG images using rich models,” Proc. SPIE, vol. 8303, p. 83030A, Jan. 2012.

[11] J. Kodovský, J. Fridrich, and V. Holub, “Ensemble classifiers for steganalysis of digital media,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 432–444, Apr. 2012.

[12] L. Guo, J. Ni, and Y. Q. Shi, “Uniform Embedding for Efficient JPEG Steganography,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, pp. 814-825, May 2014.

[13] T. Filler, J. Judas, and J. Fridrich, “Minimizing embedding impact in steganography using trellis-coded quantization,” in Proc. SPIE, Electron. Imag., Security, Forensics Multimedia XII, N. D. Memon, E. J. Delp, P. W. Wong, and J. Dittmann, Eds., San Jose, CA, Jan. 17–21, 2010, vol. 7541, pp. 05-01–05-14.

[14] C. E. Shannon, “Coding theorems for a discrete source with a fidelity criterion,” IRE Nat. Conv. Rec., vol. 4, pp. 142–163, 1959.