ISSN:0975-9646

JPEG Steganography based on uniform embedding and Syndrome trellis codes

Aasemuddin Quazi[#1], Prof. A.K. Gulve[*2]

[#] *Department of Computer Science, Government College of engineering*
Osmanpura, Aurangabad, Maharashtra, India

***Abstract*— Steganography is the art and science of concealed communication with an intention to hide the secret messages in the cover medium. The Uniform embedding distortion is used along with the syndrome trellis codes to minimize the distortion. Syndrome codes give near-best rate distortion function. Here SHA 256 hash function is used to improve the security of the image. Thus, statistical detectability will be reduced thereby improving the security.**

***Keywords*— Steganography, JPEG Steganography, Minimal distortion embedding, Uniform Embedding, Syndrome Trellis codes.**

I. INTRODUCTION

JPEG is a well-known format for digital communication and because of this reason the field of JPEG steganography is being researched on a widespread basis. The Joint Photographic Experts Group (JPEG) file format stores image data in compressed form as quantized frequency coefficients [1]. The steps for compression performed by the JPEG compressor initiates 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. Investigation of a discrete distribution of coefficients frequency of occurrence shows two features viz. 1) The coefficients degree of occurrence decreases with increasing absolute value and 2) 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].

Steganography is the science of secret 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. Usually a graphical file is used as a cover medium due to their 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 [1]. Here the intention is to reduce these distortions and also enhance the undetectability and thereby improving the security.

A method for minimising the distortion in JPEG steganography is studied here. There are two main paths for designing a steganographic scheme i.e. either design a steganographic system that preserves the cover model or design a steganographic scheme that minimise the embedding distortion.

A number of steganographic schemes have developed over the past few years, such as F5 [2], nsF5 [3], MME [4], and there are also various schemes which have been developed more recently. The main aim of these techniques was only one, minimal distortion embedding strategy, which consists of a good distortion function and a good 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 of 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 [3], the wet paper code (WPC) is used for 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 for the 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 which 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 just 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. An assumption is made here that the sender gets the payload as a pseudo-random bit stream by compressing or encrypting the original message. 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 intuitive use of steganography, since images having varying levels of noise and texture which can take varying amounts of concealed payload, for such images the distortion should be fixed instead of the payload.

II. Literature Survey

In Uniform Embedding Scheme, the sender uses a JPEG image to hide the secret message and send it to the receiver. Therefore, it becomes very hard to make a difference between the stego image and the cover image, thus it can securely send the message. The message is usually hidden in the cover by changing the elements of the cover to same extent, usually the LSB of the pixel and DCT coefficients that are quantized. In [5], the problem of decreasing the embedding impact for single-letter distortion is efficiently provided. 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,

$$D(x, y) = \sum_{i=1}^{n} \rho_i(x, y_i)$$

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 hamming codes, BCH codes and also the syndrome codes are available. The performance evaluation of these coding methods can be done using the metric of coding loss which is defined as the relative decrease in payload due to 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.

Rather than training the distortion function on a specified feature set, a universal design is made for making minimum artifacts of first and second order statistics for the function. 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 embedding the payload in the JPEG image, the DCT coefficient might be changed to some point, which may be 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. Therefore the modifications produced by the message embedding in PDF can be stated as

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

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].

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

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,

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

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].

In minimizing additive distortion in steganography using syndrome trellis codes, a full practical method is given. 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.

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.

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.

The SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. The SHA-2 family uses an identical algorithm with a variable digest size SHA-256 .it is believe the most secure hashing algorithm as this article is written, here are few examples for the SHA implementation. The possible Message Digest algorithm are SHA-256,you can check the reference for the detail.SHA-2 is believe the most secure hashing algorithm as this article is written, here are few examples for the SHA implementation. The possible Message Digest algorithm are SHA-1, SHA-256, SHA-384, and SHA-512, you can check the reference for the detail .This Message Digest class provides applications the functionality of a message digest algorithm, such as SHA-256. Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.

III. PROPOSED SYSTEM

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 every 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. 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. Using the number of rows and columns of the stego image, the

splitting of the stego image is done. 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.

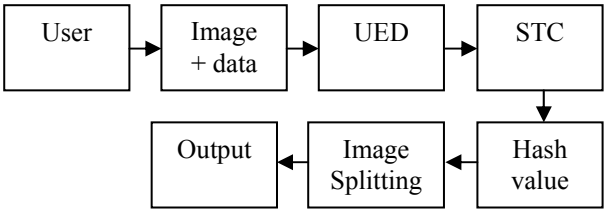

Fig. 1 Proposed Scheme

The complete functioning of the project is modularized into four parts viz. User interface, Steganography module, Generating hash value using SHA 256 module & Stego image splitting module. In the user interface module, a web interface is provided by using the java technology. JSP pages provide the main interface and servlets are used to handle the requests and process them. To perform steganography user has to login using an ID and password which can be created by signing up. Only those users who have a valid ID and password can perform the intended operation. The interface also provides a window for selecting the image on which steganography is to be performed.

For deciding the embedding capacity of an image it has to be made sure that the message hidden is not detectable and minimum distortion is also achieved. For uniformly embedding the message a technique called Permutative Straddling [15] is used. This technique is used for calculating pseudo random permutation for which the coefficients are used for embedding messages. Running out of symbol probabilities before running out of bits infers that maximum message length for the image is achieved. Maximum length is attained by calculating the entropy of symbol frequency. Here an auto generated message of maximum length possible is provided to be embedded into the image.

After this a hash value is generated for the stego image. The hash value is generated using the SHA-256 algorithm. SHA stands for Secure Hash Algorithm. The hash function runs on digital data and gives a hash value for that data. Hash values are mainly used for verifying data's integrity. Here the stego image is passed to the receiver using mail, so SHA 256 serves best for securing the stego image during its transmission. The receiver can check the hash value of the received image with the previously calculated one to determine whether it has been tampered or modified. This adds to the security of the proposed scheme. The main advantage of hash function which makes it so much secure is their 'collision resistance': which means no one should be able to find two different input values that gives the same output. The Fig. 2 below shows the snapshot of hash value generated for the stego image,

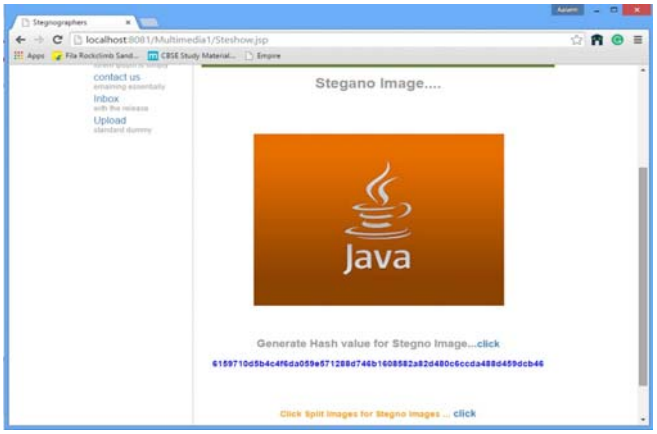

Fig. 2 Snapshot of hash value generation

After generating the hash value the next thing done is splitting the image based on rows and columns. The major advantage of splitting the image is to provide security. Here only one part of the splitted image is send to the receiver. So even if the adversary gains access to the stego image he won't be able to obtain the complete message. Thus by splitting the image the security is further enhanced. The Fig. 3a & 3b below shows a snapshot of image splitting. As it can be seen that the image is split into four parts and only one part is send to the receiver. The selection of the part of the image to be sent is independent for the user. The range for splitting is 1 – 9.

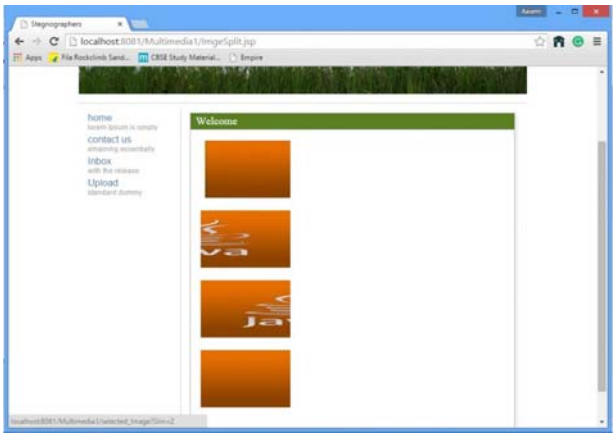

Fig. 3a Image Splitting

Fig. 3b Sending splitted Image

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,

$$Ext(y) = Hy = m$$

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,

$$Y = Emb(x, m) = arg \min_{z \in C(m)} (D(x, y))$$

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

IV. Results

As a performance measurement for image distortion, the well-known Peak-Signal-to-Noise Ratio, PSNR, which is used under the difference distortion metrics, can be used for the stego-images. It is defined as:

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE}$$

where MSE denotes the Mean Square Error between the original image and reconstructed image. For an N x N image, its MSE is defined as:

$$MSE = \left(\frac{1}{N}\right)^2 \times \sum_{i=1}^{N} (x[i, j] - \hat{x}[i, j])^2$$

Here X[i , j] and X'[i , j] denote the original and decoded gray levels of the pixel [i , j] in the image respectively. A larger PSNR value means that the stegoimage preserves the original image quality better. PSNR values falling below 30dB indicate a fairly low quality i.e. the distortion caused by embedded image is detectable.

Given below are the cover image and the stego image obtained by using the proposed scheme.

Fig. a Cover Image

Fig. b Stego Image

The histogram for the cover image and stego image is given below,

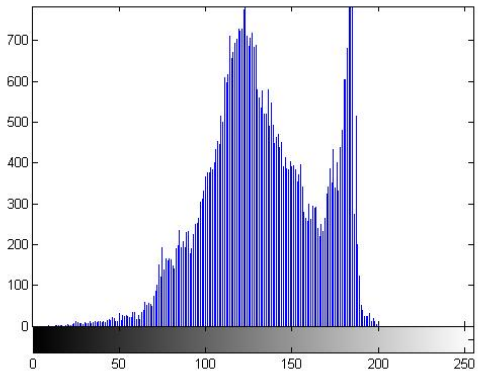

Fig. c Histogram of cover image

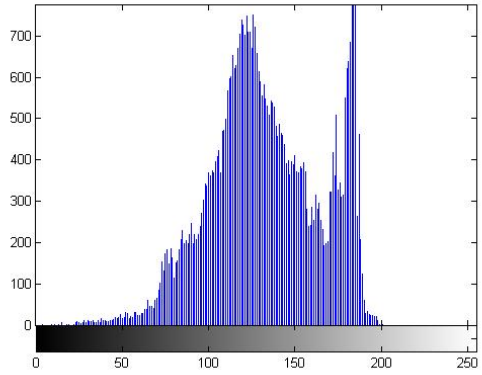

Fig. d Histogram of stego image

As it can be seen from Fig c & Fig d, there has been very less distortion between the cover image and the stego image. The size of the cover image is 4541 bytes and the data entered is 862 bytes. After entering the maximum possible message length, the PSNR value achieved by using the proposed scheme for the above image is 41.316

V. CONCLUSION

The minimal distortion embedding scheme provided here can be practically implemented for achieving high embedding efficiency for JPEG steganography. This JPEG steganographic scheme is made efficient by combining Uniform embedding scheme (UED) and Syndrome trellis codes (STC). 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.

REFERENCES

[1] Aasemuddin Quazi and A.K. Gulve, "A review on Uniform embedding for efficient JPEG Steganography," International Journal of Computer Application, vol. 114(12), March 2015, pp. 19-23

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

[3] 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.

[4] 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

[5] 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.

[6] 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.

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

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

[9] 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.

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

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

[12] 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.

[13] 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.

[14] 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.

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

[16] Steganography software for Windows, http://members.tripod.com/steganography/stego/ software.html 2002.