Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 4, Issue 4, July 2020

Reducing Distortion in Steganography using Syndrome Trellis Code

Bhavya K S
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India

Deepika H V
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India

Harshavardhini V Patil
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India

Yeswanth Reddy K
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India

Latha B N
Assistant Professor, Dept. of ECE, JSSATE, Bengaluru, India

Dr. Sathish Shet K
Assistant Professor, Dept. of ECE, JSSATE, Bengaluru, India

Abstract: Data protection is one of the most daunting issues facing the technology world today. Numerous schemes have been proposed over the last decade to protect the transmission of confidential data over the public network (Internet). Steganography, along with cryptography, can be one of the best ways to solve this problem. The word stego is the Greek word "Secret." Steganography is the process of embedding a hidden message to an image. Essentially, distortion occurs as pixel length increases, as distortion increases hackers can easily target the computer and can easily view the information contained in the image. The non-binary embedding scheme by syndrome-trellis codes is used here to reduce the distortion. The role of the Trellis Syndrome Code in steganography is to assign a scalar to any possible value of a stego element representing the distortion of an embedding shift by replacing that value with the cover element. The entire distortion is assumed to be a portion of the pre-element distortions.

Keywords: Steganography; Syndrome Trellis Code; Distortion

I. INTRODUCTION

Web users are expected to store, receive, or send information periodically. The most regular way of doing the process is to transform the knowledge into another form. Only those who know how to restore it to its original content will understand the data resulting therefrom.

This method is called as encoding or encryption. One of the big drawbacks of encoding is that it doesn't disguise information existence. Although the data encoded is illegible. It still exists in data form. If adequate time is granted, the data can eventually be decrypted by anyone. This can be solved by steganography. Steganography is the art and science of concealing knowledge, and a steganographic scheme blends confidential material into unremarkable cover media in order to avoid raising the suspicion of an eavesdropper. People used secret tattoos or translucent tin beforehand for the steganographic data transmission. The computer and network technologies provide the steganography system with easy-to-use communication networks.

In essence, the method of information hiding begins with a steganographic approach by removing obsolete data bits from the cover medium (which can be altered without losing the medium integrity). Syndrome, embedding creates a stego medium by substituting certain redundant data bits for the hidden data message. Syndrome Trellis Codes are basically binary linear convolution codes described by the quest for matrix parity. This representation allows it to be used where channel code is not required to troubleshoot data. Therefore steganography is the case.

II. LITERATURE SURVEY

Reference [1] suggests that Steganography is widely classified on the basis of Spatial-domain and transform-domain. The hidden messages are specifically located within the spatial domain. By changing the cover image's Gabor coefficients the steganography scheme embeds the secret message. The data hiding technique using DWT was executed on both the hidden and the cover images. The secret message can be found in the high frequency coefficients performed on the cover in DWT. Recently the data hiding method has become important in many areas of application.

Reference [2] suggest that the technique of steganography, cryptography and digital watermarking is used to provide data security. Steganography, by applying Steganography methods, is a form of hiding data within other data such as cover medium. Cryptography and digital watermarking make human data unreadable known as cipher so that cryptography scrambles messages. Whereas steganography contributes to abuse of human awareness in such a way that it remains undetected or intact. All computer media, digital data or files may be used as a covers tool for steganography.

Reference [3] suggests that the objective of this venture is to use steganography to obtain secure encryption and authentication. In order to accomplish this, numerous organizations and universities around the world have provided solutions for secure communication, many algorithms have been created in the meantime, including AES, RSA, and LSB etc. But although these algorithms have been developed, hackers have been subjected to a breakdown that makes them obsolete.

It was attempted to merge several existing algorithms such as AES, LSB into one proposed system. Next, the use of steganography is introduced in the proposed system along with conventional encryption. Second, we're trying to get user authentication via e-mail using OTP. Second, the encrypted data is split and sent across many servers so that full encrypted data cannot be accessed in one direction. The likelihood of data leakage becomes very small and very difficult to hack by applying the proposed model.

Reference [4] suggests Error correcting codes have been widely used for information hiding in two aspects secret message protection and syndrome coding. The former concentrates on robustness enhancement often embedded data. In BCH codes and repeat accumulate codes are employed to encode the embedded data for resisting active-attacks or channel disturbance respectively. While the latter places emphasis on solving the impact minimization problem. Syndrome coding, also known as matrix embedding, an embedding method with the cover coefficients perturbed minimally.

In general, the embedded data falls within a coset of the adopted error correction language. Several schemes based on the same principle have been suggested, based on different types of Golay codes, BCH codes, random linear codes, and convolutional codes. These include the state-of-the-art trellis syndrome codes (STCs), implemented by the Viterbi algorithm on the structure of the syndrome trellis of convolutional codes and able to perform close to the bounds derived from sufficient rate-distortion bounds. Due to its outstanding performance it was adopted as the core algorithm in the popular steganographic tool-HUGO.

Reference [5] suggests Steganography is the manner in which messages are hidden in a media. So there may be no ability to recognize the presence of contact. Steganography contrast with cryptography in which the message can be examined and altered against certain privacy goals provided by the cryptographic algorithms, in steganography the message is hidden within another message that hides the actual message's existence.

Steganography can be used with various media types. The media in its digital form can be anything like audio, video, picture, text, network protocol etc. These can be known as cover object and after the covering process it is called as stego-object. Steganography is the method of hiding data, i.e. the actual data is not updated, but the information is concealed in the information about the carrier. A key is often used to restrict the identification of the hidden data from external parties. Steganography has broad range of applications particularly in the area of internet where security and privacy are very significant factors.

III. METHODOLOGY

In the language of information theory, STCs include a fidelity criterion (also referred to as the binning issue) tools to solve the source code problem Here we can find the implementation of the Syndrome-Trellis Codes (STCs) in MATLAB.

The two approaches are used to hide or secure sensitive data in the cryptography and steganography. However, both vary in that cryptography makes the data unreadable or hides the purpose of the data while steganography hides the presence of the data. Cryptography is also used to complement the steganography protection offered. Algorithms for cryptography are used to encrypt sensitive information. Cryptography algorithms are used to encrypt confidential information beforehand it is embedded in the cover films.

The only benefit of cryptography is that the intended secret message does not draw attention to itself. Clearly readable encrypted texts are troubling and can be intrusive in countries where encryption is forbidden, no matter how unbreakable they may be. In other words, steganography is more secure than cryptography to send confidential information.

The disadvantage of existing systems is that there is more distortion in the image, less message is embedded, and less security. The current paper addresses these drawbacks of the current framework. The LSB technique has been used to embed our message in the image.

Computerized steganography has recently become very common. Hidden messages can be contained in digital data such as.jpg, .png images, audio files, or e-mail messages using a number of encoding methods. These strategies are described below. In this way, the authors are prepared to watermark their property. Terrorist groups all over the globe. Most of the content of the adaptive steganography approaches now currently focused on a model of minimizing distortion between the cover and the corresponding stego component.

A. *Advantages of the Proposed System*

- Minimizing additive distortion in image.
- Security is more and more message is embedded comparatively existing system.

B. *Image Steganography*

Data Steganography refers to a method of removing data from image files. Of this reason, the image chosen is called the cover image, and the picture obtained after the steganography is called the stego image.

C. *Block Diagram of Proposed System*

Fig. 1 describes the block diagram of an implementation of the proposed system. A cover picture implies that a picture taken to insert a message is given as an input 'X' with the message 'M' and the main 'K' is inserted in the stego dimension 'Y' and transmitted via the stego channel. The function of embedding is that the LSB of the picture pixels can be modified pseudo-randomly on the spatial domain.

This has other benefits, such as higher size, image consistency and low computing difficulty. The extraction algorithm is that it subtracts a secret message from a cover message. To retrieve the message from the picture that is obtained from the sender, one should have the key that is used during the embedding of the document. Here “X” and “Y” are random variables on image function.

This will be done by comparing the cover image, plotting the histogram, or detecting noise. Even though efforts are being made to create new algorithms with greater immunity to these attacks, efforts are also being made to strengthen current steganalysis algorithms to detect the sharing of sensitive information between terrorists or criminal elements.

D. *Syndrome Trellis Code*

The purpose of the Syndrome-Trellis codes is to assign an embedding distortion on each cover item and then embed as little distortion as possible on a similar bundle. Integrated mapping and extraction shall be described as,

$Emb\{0,1\}^n * \{0,1\}^k \rightarrow \{0,1\}^n$, and

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

$Emb(x,m) = y, \forall x, y \in (0,1)^n$

$Ext(y) = m, \forall m \in \{0,1\}^k$

The message chain is m, where the cover vector is x and the stereo vector is y. The approach should modulate the k-bit message in the n-element cover, while keeping as small as possible the distortion required. For syndrome-trellis encryption, embedding and abstraction is done using a linear binary code C of length n and dimension n-k. As H is its set, its parity-check vector, the extraction mapping is

$$Ext(y) = Hy = m \qquad (1)$$

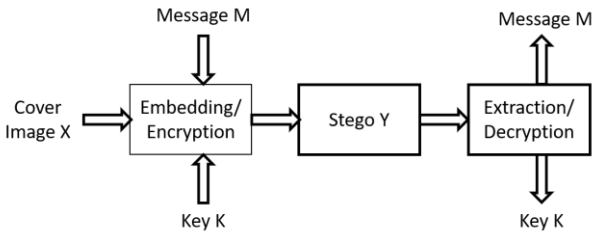

Fig 1. Overview of proposed system

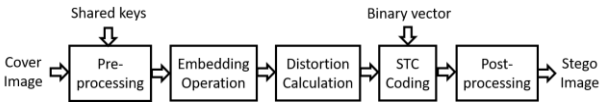

Fig 2. Block diagram of Encryption

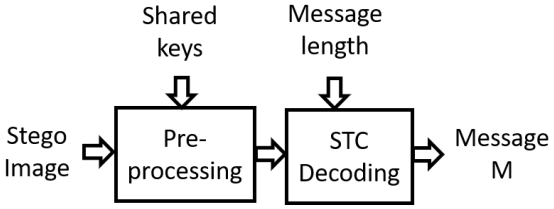

Fig 3. Block Diagrams of Decryption

Suppose $C(m) = \{z, \{0,1\}^n \text{Hz} = m\}$.

The STC method takes the ideal z nearest to x from the coset C (m) as output y, unless the coset refers to the message sequence m,

i.e., $Emb(x, m) = \text{argmin}\big(D(x, y)\big)$ (2)

Filler et al. gave the syndrome-trellis strong design and implementation codes. It should be recalled that the STC could very easily increase the embedding efficiency at low embedding speeds. At a rapid point of integration, though, its development will be minimal.

E. LSB Embedding Operation

The most widely used way of covering data is to use the LSB. While there are some inconveniences to the present method, the relative simplicity of its implementation makes it a well-liked operation. To cover a hidden message inside a frame a correct cover image is needed. Since this approach uses bits of pixel within the image, a lossless compression format is required, otherwise the hidden information will wander within a loss compression algorithm's transformation. When using a 24-bit color image, a touch of each of the red, green, and blue components is often used, so that a full three-bit image is always stored in each pixel. Therefore, an image of 800 to 600 pixels will contain a complete sum of hidden data of 1.440.000 bits (180.000bytes).

F. LSB Encoding Algorithm

The hidden data is embedded into an image using LSB Encoding. The inclusion of LSB enables a large amount of secret information to be used by replacing the LSB of each sampling bit with binary data. First take the initial photo, then encrypt the hidden message. The secret data encrypted is then converted into binary format. It is in America that binary conversion is done. The binary conversion occurs via the American Standard Information Code.

Interchange the character values (ASCII) and convert them to a binary format and generate a stream bit. Similarly, pixel bytes are recorded in a single array, and byte streams are generated in the cover image. Message bits are sequentially taken and inserted into LSB file fragments. Despite this approach. This approach is followed until the picture bytes contain all bits of the message. The created image is therefore called "Stego-Image."

G. Encoding Algorithm

Step-1: Read the cover image and the secret text information to be incorporated into the image of the cover.

Step-2: Should be resized to cover image.

Step-3: After resizing the image should be divided into 3 colors and one color is selected to hide the data.

Step-4: The process of segmentation applies to image, the process of dividing an image into segments. A lot of segmented image is formed out of the image.

Step-5: For every segmented image histogram is checked, it is the process of finding a maximum noise in segmented images that is by calculating non-zero element, where there is more non-zero element there the noise is more. So in that segmented image data can be hidden.

Step-6: The Trellis Code technique is used to insert the data into the segmented image where the image is transformed into a parity matrix, the data is translated into binary format, and the last pixel of the segmented image is added to the image.

Step-7: The cover image will be transformed into a stego image before the data is inserted, and on the side of the encryption the key is produced.

Step-8: Continue the procedure until the cover paper completely conceals the confidential details.

H. LSB Decoding Algorithm

First, Stego-Image is taken and a single byte array is created, as happened during the encoding. Take the total number of hidden bits and bytes with encoded information representing stego-image pixels. Initially, the counter is set to 1, which effectively implies the index number of pixel bytes where the LSB accesses the hidden message bit. A loop continues until a fragment of the hidden message hits the final count. Before that the message's bit stream is produced. Open bits are clustered to form bytes of a single ASCII character in each packet. Characters are stored in a text file containing an encoded message which is encrypted. After this there will be decryption and decompression.

I. Decoding Algorithm

Step-1: Read the stego image.

Step-2: Split the stego image into three colors, i.e. red, green and blue (RGB).

Step-3: The process of segmentation applies to the stego image.

Step-4: Histogram is checked to the segmented image to find a maximum noise to find the segmented image where there is a data.

Step-5: The difference of stego image and key results in data.

Step-6: The binary format data is converted into actual message format.

Step-7: Reconstruct the secret information.

IV. RESULTS AND ANALYSIS

The proposed system using MATLAB for various types of images is illustrated and the below description highlights all the possible validation of the proposed system and it has been compared with the performance metrics like PSNR and MSE.

Demonstrating the effectiveness of the proposed method by considering a jpg image as a cover image and applying a segmentation process to the cover image after resizing the cover image. After the histogram has been tested, the data is concealed inside the segmented image. Thus a stego image is generated and the key is produced in the encryption. Key is obtained by adding the segmented images. Here some function files are included along with the built in file as shown in the code. The same key is used in decryption side to get the data from the stego image. The data can be obtained by distinguishing between the stego image and the logo.

A. *Cover Image*

Cover Image- An image of size 676 * 538 which is of .jpg format.

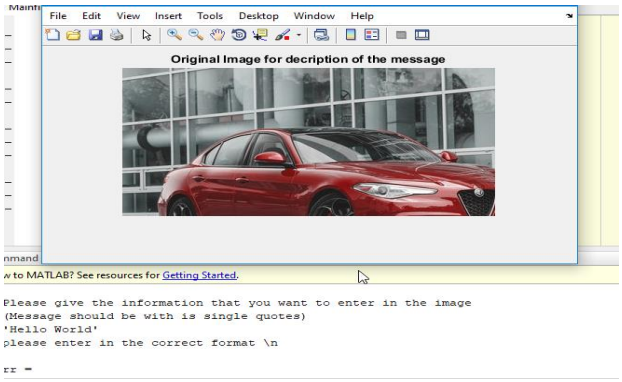

Fig 4. Cover Image

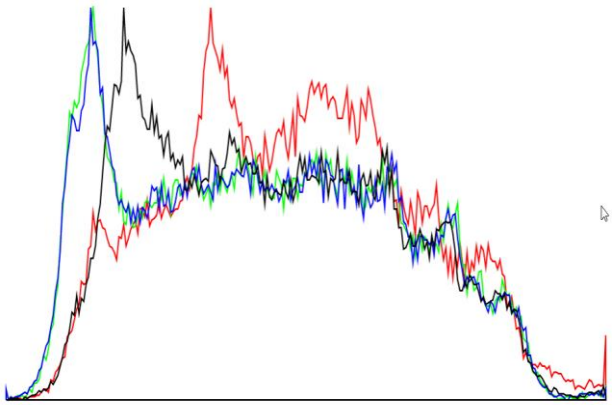

Fig 5. Histogram of Cover Image

Figure 4 and 5 shows the image cover and histogram which is an image taken to hide the details. The file size of .jpg format and its resolution is 678 * 538. The overall distortion of the cover image histogram.

B. *Stego Image*

The image on which the data embedded in this image is concealed is "Hello World," shown in Figure 8.

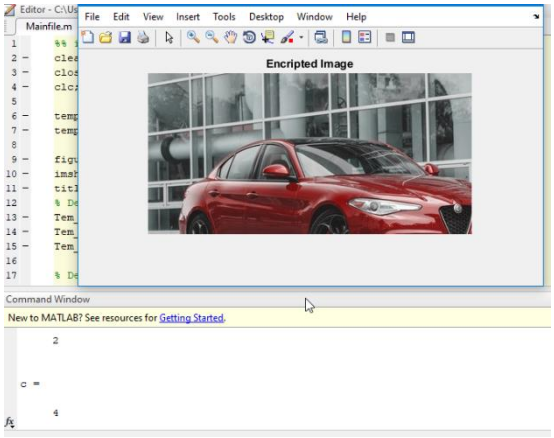

Fig 6. Stego Image

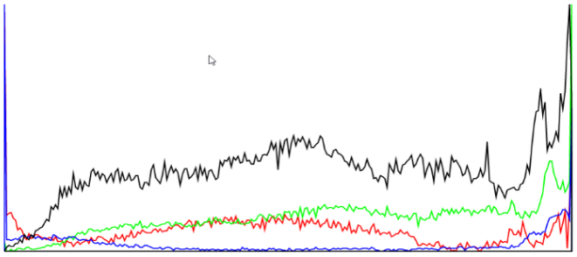

Fig 7. Histogram of Stego Image

Figures 6 and 7 show a stego image and its histogram where the data is hidden, the image that is obtained after an encryption algorithm has been applied. The histogram of stego image is where the distortion is minimized as observed in graph after applying a syndrome trellis code.

When comparison is done between the cover image and stego image in terms of histogram, there is a decrease of distortion in stego image. Here the data to be embed is enter in the stego image.

C. *Output of the Image*

The data which is decrypted from the stego image.

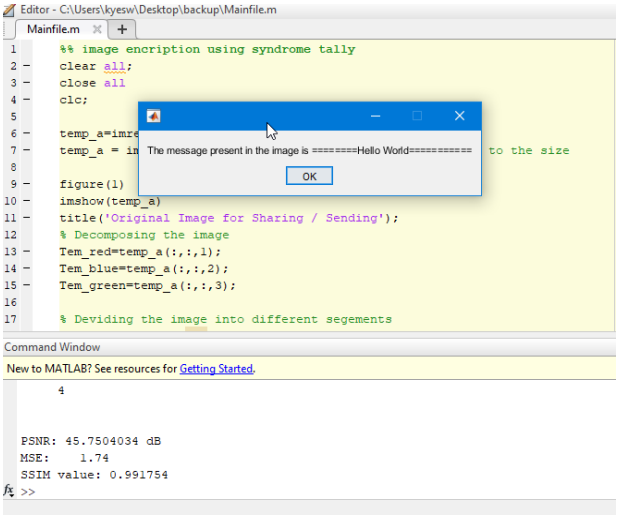

Fig 8. Output of the Image

Figure 8, obtained after the decryption algorithm applied to the stego image, shows the message embedded in the stego image by applying the key to the segmented image, the resulting difference. It may be noted that the message entered in Figure 8 is shown.

Image Name	Image Capacity	MSE	PSNR(dB)	SSIM
Car.jpg	676 * 538	1.74	45.7504034	0.989005
Nat.jpg	663 * 510	1.95	45.2578510	0.991983
Im.jpg	655 * 499	1.60	46.1148771	0.994424
Road.jpg	763 * 522	1.95	45.2609324	0.991754
Ia.jpg	275 * 183	1.79	45.6439183	0.981980

Table 1. Values of MSE, PSNR and SSIM for different images

The MSE, PSNR, and SSIM values are shown in Table 1. The performance indicators that are used to inspect the image quality after hiding the data. Since the image quality does not change after deletion of the data. The values of MSE, PSNR and SSIM have been checked for various image sizes and the values remain almost constant. Therefore it can show that after embedding the data in the respective images, the quality remains constant.

Image Name	Image Capacity	MSE	PSNR (dB)	SSIM
Car.jpg	676*538	1.78	45.6633653	0.988984
Nat.jpg	663*510	1.78	45.6639757	0.878983
Im.jpg	655*499	1.78	45.6680472	0.989069
Road.jpg	763*522	1.79	45.6435538	0.989013

Table 2. Values of MSE, PSNR and SSIM when message length is increased

Table 2 reflects the MSE, PSNR, and SSIM values that are obtained as the characters in the image increase. Thus it shows that while the length of the message is changed, the quality of the images remains unchanged.

V. FUTURE SCOPE

The proposed method helps the data which is embedded in the image to be confidential so it can be used for military purposes to send and receive data among themselves

VI. CONCLUSION

This functions as a better way to encrypt a hidden message than an encryption that disguises only the background message, rather than the meaning of the message. The defects in the picture are reduced, the message is not clearly perceptible and thus attackers cannot detect it. These methods are not limited to binary embedding operations and enable the embedder to dynamically select the embedding amplitude modifications that are based on the cover image information. The need for the receiver to share the defect function, or the embedding process. They can also transform picture to picture, in fact. Last but not least, the architecture is not limited to embedding with greater amplitudes but can be used, for example, to embed color images. The three-color LSBs can be interpreted as three-bit symbols representing cost functions.

ACKNOWLEDGEMENTS

We thank his holiness Jagadguru Sri Shivarathri Deshikendra Mahaswamiji for his blessing to this venture. We would like to thank Mrs. Latha B N, Assistant Professor and Dr. Sathish Shet, Assistant Professor, Department of ECE, JSSATE-B for their inspiration, supervision, kind assistance and guidance. Their trust and confidence in our abilities were the driving force to complete this paper.

REFERENCES

[1] Naveen Chandra Gowda ,P. Sai Venkata Srivastav, GuruPrashanth R,Raunak.A,Madhu Priya R, ”Steg Crypt Encryption using steganography” IJEAT Volume-8 ,Issue-5S, May 2019.

[2] Xueyi, Lu Guopeng, Wang Yunlu, Zhang Yan,” A JPEG Steganographic method based on syndrome Trellis Codes” IJERT 10th January 2013.Vol.47 No.1.

[3] Tomas Filler, Jan Judas, Jessica Fridrich "Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization", January 18-20, 2010.

[4] P N S Lakshmi, Ch N P Latha,”A Novel Syndrome Coding Scheme For Embedding And Minimizing Distortion in Steganography” IJCSMC, Vol 2,Issue.10,October 2013.

[5] Rupali Bharadwaj, Vaishali Sharma,”Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution” ICACC, September 2016.

[6] Guangjie Liu, Weiwei Liu, Yuewei Dai, Shiguo Lian,”Adaptive Steganography Based On Syndrome- Trellis Codes and Local Complexity” IEEE, June 2012.

[7] Sravanthi, Ramesh.J, Naresh.A, "Improved Statistical Steganalysis Using Syndrome-Trellis Codes" JATIT Vol. 1 Issue 6, August – 2012.

[8] M.Suryadevi, S.Thenappan, "Uniform Embedding For Efficient JPEG 2000 Steganography - Syndrome Trellis Coding" ISO, May 2015.

[9] C.P.Sumathi, T.Santanam, G.Umamaheshwari "A Study of Various Steganographic Techniques Used For Information Hiding" IJCSES, Vol.4, December 2013.

[10] Swasti Saxena, "Secure Data Transfer through a Combination of Steganographic and Cryptographic Encryption Technique", Feb 2015.

[11] Michael T Raggo and Chet Hosmer, "Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols" 1st Edition.

[12] Eric Cole," Hiding in Plain Sight: Steganography and the Art of Covert Communication".

[13] L.Zhang, X.Zhao, "An Adaptive Video Stagenography Based on Intra-Prediction Mode and Cost Assignment" IEEE, May 2007.

[14] C. Wang, J Ni, "An Efficient JPEG Steganographic Scheme Based on the Block Entropy of DCT Co efficients" May 2012.

[15] Y.Dong, X.Jiang, T.Sun, D Xu, "Coding Efficiency Preserving Steganography Based on HEVC Steganographic Channel Model" IEEE, April 2007.