A Novel Steganography Scheme for Color Image Based on HLS Translation

Guoqiang Shao¹, Longmei Jie²* and Dan Shen²

¹Computer Science & Information Technology Collage, Daqing Normal University, Daqing 163712, Heilongjiang, China
²College of Electrical Engineering, Yingkou Institute of Technology, Yingkou, Liaoning 115000.
Email: 343649787@qq.com

Abstract. In recent years, steganography has attracted extensive attention, but most of steganography schemes are aimed at grayscale images. Therefore, a novel steganography scheme for color image based on HLS translation is proposed in this paper. Firstly, the color cover image is decomposed from RGB three channels to HLS three channels. Then the image of H channel is selected as the cover image for embedding secret information due to its texture feature of original image. The universal distortion function UNIWARD is utilized to embed the secret information into the image of H channel. Finally, the steg image transmitted in common channel is obtained by inverse HLS transform using the single channel image embedding the secret information. The extensive experimental results indicate that our scheme has high security and can also resist the detection of steganalysis schemes based on CNN.

Keywords. HLS translation; steganography; high security; CNN.

1. Introduction

With the continuous development of Internet technology, information acquisition has become more and more convenient, followed by massive data can be stored and transmitted on the network without restriction. The Internet not only brings convenience to our life, but also increases many security risks. Lawless elements can use the public networks to spread some harmful information, propaganda bad speech and so on. However, with the popularity of Internet, steganography has gradually entered people’s field of vision [1, 2]. Steganography focus on embedding secret message into the cover image without affecting the appearance of the cover image and is used for covert transmission. There are two fundamental components in steganography: transmission cover and secret message [3]. For image, it already contains a lot of characteristic information, such as pixel brightness value, color, texture feature, edge and high-level semantics, therefore, it is very suitable as the transmission cover. The secret message can be text, image even video, etc.

Currently, most of steganography methods use grayscale image as cover image, which is difficult to achieve in real life. Fridrich et al. [4] determined the capacity of JPEG images by testing the best steganography methods. The grayscale JPEG images were selected as cover images to embed with different payloads in their experiments. They also did a lot of experiments by adjusting the different designing details to observe the impacts on steganography schemes. Golgan et al. [5] proposed a perturbed quantization steganography using wet paper codes. In their scheme, the secret information can be hidden during the process of lossy compression, A/D translation, etc. The grayscale image also was chosen as the cover object element. Filler et al. [6] presented a gibbs construction in steganography,
which connected the steganographic design with statistical physics to minimize the embedding distortion. Li et al. [7] proposed a novel steganography method using chaotic encryption technology and generative adversarial networks, which not only enhanced the security of steganography but also increased the embedding capacity. Both the secret message and cover image selected the type of grayscale image in their experiments. More than that, many traditional steganography methods, the cover images are grayscale, such as HUGO [3], WOW [8], UNIWARD [9], etc. In fact, color images are widely used in real life, while grayscale images are rarely used.

In order to introduce color image into the traditional image steganography and ensure the security, a novel steganography scheme based on HLS translation is proposed in the paper. Firstly, the color cover image is decomposed into RGB channels to obtain three grayscale images. As we all know, the texture region of images is the most insensitive region of human sensory system, and it is the most difficult part to be detected for steganalysis. So the proposed method converts the RGB cover image into the HLS space and chooses the image of H channel as carrier of embedding secret message due to its rich texture features. Secondly, the universal wavelet relative distortion (UNIWARD) is utilized to embed the secret information into the selected carrier. Finally, the image of H channel with secret message is used to do the inverse HLS translation to obtain the color cover image transmitted in public channel. The receiver can do the same operation to get the transmitted secret message.

The specific architecture for the rest of this paper is as follows. Section II introduces the recent developments on steganography and steganalysis. The details of the proposed method are explained in Section III. The experimental results and analysis are discussed in Section IV. Section V gives the conclusion of our steganography method.

2. Related Work

2.1. Image Steganography

Currently, the commonly image steganography methods mainly include spatial steganography and transform domain steganography. The spatial image steganography focus on embedding the secret message by directly modifying the pixels of cover image, including least significant bits (LSB), WOW, HUGO, etc. In the spatial domain, the cost of embedding is usually lower in the area of texture but higher in the smooth region. For example, HUGO [3] defines the specific distortion as the weighted form between the high-order statistics that pixel difference between cover image and steg image. In this definition, the higher weights are assigned to the well-filled storage bins and the lower weights are assigned to the sparse storage bins corresponding to the more complex regions. Another model-free approach, call wavelet obtained weights (WOW) [8], uses a set of directed high-pass filter to obtain what is known as the directional residuals. There are other distortion functions, of course. The distortion function, called UNIWARD [9], is similar to WOW’s design but simpler and suitable for embedding any domain. Figure 1 represents the traditional steganography architecture.

![Figure 1. The sketch of traditional steganography model. Sender: the embedding algorithm is utilized to embed the secret information into the cover image to obtain the steg image without damaging the appearance of cover image. Receiver: the secret information can be extracted using the extracting algorithm. Note: The steg image transmitted in public channel may be detected by the steganalysis technology.](image-url)
2.2. Image Steganalysis

Please ensure that affiliations are as full and complete as possible and include the country. In contrast to the image steganography, the technology of steganalysis focus on detecting the presence or absence of secret information hidden in the cover image. Traditional steganalysis technology is to design specific filter to artificially extract features, which can be utilized to detect or identify the secret information in the transmitted image [10]. Currently, CNN can achieve start-of-art performance for the task of compute vision. Researchers have also found that CNN is very suitable for image steganalysis, and can achieve start-of-art experimental effect. Tan and Li et al. [11] proposed a steganalysis system based on CNN, which is formed a stack of convolutional auto-encoders. Its performance is better than the conventional SPAM method, but still lower than the conventional SRM method. Qian et al. [12] presented a new idea for steganalysis to learn features automatically via deep learning algorithms. Xu et al. [13] proposed a CNN architecture, which consists of batch normalization and 1×1 convolutional layers. The extensive experimental results have indicated that XuNet has a good steganalysis ability, which is comparable to the traditional steganalysis methods. Ye et al. [14] proposed a CNN architecture named YeNet, in which the following aspects are considered: the awareness of selection channel, the amount of high-pass filters and the blocked linear elements, and. Li et al. [15] presented a spatial steganalysis system based on CNN with parallel subnets. Steganalysis and image steganography are developing together. Only with the confrontation of steganalysis technology, the development and progress of image steganography can be better promoted.

3. Proposed Approach

In order to convert steganography from grayscale images to color images, while ensuring the security of secret information during the process of transmission, this paper presented a novel steganography scheme based on HLS translation for color image. Not like the traditional steganography methods, firstly, the color cover image is divided from RGB channel into the HLS channel to obtain the three grayscale images. Then The universal distortion function UNIWARD is utilized to embed the secret information into the image of H channel. Actually, the image of H channel has the most of texture features of original color cover image, so choosing the image of H channel has high security. The steg image transmitted in common channel is obtained by inverse HLS transform using the single channel image embedding the secret message. The receiver can do the same operation to get the transmitted secret message. The overall architecture of the steganography system proposed can be reflected in figure 2.

![Figure 2](image-url)  
**Figure 2.** The sketch of traditional steganography model. **Sender:** the embedding algorithm is utilized to embed the secret information into the cover image to obtain the steg image without damaging the appearance of cover image. **Receiver:** the secret information can be extracted using the extracting algorithm. **Note:** The steg image transmitted in public channel may be detected by the steganalysis technology.
3.1. HLS Translation for Color Cover Image

Due to the high balance and correlation among three color components in RGB space, embedding secret information into any component of the color image can seriously affect the appearance of the color image, which lead to distortion and arousing suspect of attacker. As we all know, HLS color space is more intuitive to human visual system, where H, S, L represent hue, saturation and lightness, respectively. It can be concluded from our experiments that H components occupies most of texture features of original color image, so it is very suitable to be used as cover for embedding secret information. So, we convert an image from RGB color space to HLS color space. The operated rules of three components are shown as follows.

\[ H, S = 0 \] \hspace{1cm} (1)

with

\[ \text{min} = \text{max}, \text{where} \quad \begin{cases} \text{min} = \text{min}(R, G, B) \\ \text{max} = \text{max}(R, G, B) \end{cases} \] \hspace{1cm} (2)

The L components can be computed by using equation (2).

\[ L = \frac{\text{min} + \text{max}}{2} \] \hspace{1cm} (3)

The H component and S component correspond to different calculations depending on the L component. The specific calculated details for S component are shown as follows.

\[ S = \begin{cases} \frac{(\text{max} - \text{min}) \cdot (2 \cdot \text{max} - \text{min})}{\text{max} - \text{min}, L > 0.5} \\ \frac{(\text{max} - \text{min}) \cdot (\text{max} + \text{min})}{\text{max} - \text{min}, L \leq 0.5} \end{cases} \] \hspace{1cm} (4)

From our experiments, the H component includes most of texture features of original cover image. The specific calculated details for H component are shown as follows.

\[ H = \begin{cases} \frac{(G \cdot B)}{\text{max} - \text{min}} \cdot 60, R == \text{max} \\ \frac{(2 + (B \cdot G))}{\text{max} - \text{min}} \cdot 60, G == \text{max} \\ \frac{(4 + (R \cdot G))}{\text{max} - \text{min}} \cdot 60, B == \text{max} \end{cases} \] \hspace{1cm} (5)

In this paper, the H component in HLS color space is selected as cover for embedding secret information. The specific reasons are as follows. Firstly, the HLS model is composed of double pyramid, which can reflect the different features of the color image from the aspect of design. Then the H component includes most of texture features of original cover image. As we all know, the operation of embedding secret information into the edge or texture region of image can resist the detect of steganalysis algorithms without damaging the appearance of cover color image.

3.2. Embedding Algorithm for Secret Information

In this paper, the universal wavelet relative distortion (UNIWARD) is utilized to embed the secret information into the selected image of H channel. The UNIWARD can embed secret information into the edge or noise region of cover image to avoid detect of steganalysis algorithms. In their hiding method, the most popular steganographic method is followed. A suitable distortion function is defined when the secret information is embedded, as shown in equation (6).

\[ D(X, Y) = \sum_{i=1}^{H} \sum_{j=1}^{W} \rho_{i,j} | x_{i,j} - y_{i,j} | \] \hspace{1cm} (6)

where X and Y represent the cover image and steg image, respectively. The size of all images is H×W. \( \rho_{i,j} \) represents the cost of \( x_{i,j} \) changes to \( y_{i,j} \) when embedding secret information. The UNIWARD
introduced a directional filter bank into the construction of distortion function. The specific definition of UNIWARD is shown as equation (7).

\[
D(X, Y) = \sum_{k=1}^{3} \sum_{u=1}^{n} \sum_{v=1}^{n} \frac{|W^{(k)}_{uv}(X) - W^{(k)}_{uv}(Y)|}{\sigma + |W^{(k)}_{uv}(X)|},
\]

where X and Y also represent the cover image and steg image. The different W(X) and W(Y) can be computed by the \( u \)th wavelet coefficient in the \( k \)th subband of the first decomposition level, \( k=1, 2, 3 \) and \( u \in \{1, ..., n_u\}, v \in \{1, ..., n_v\} \). Please note that \( \sigma \) is a contrast of stable numerical calculation and it is generally taken as a value of greater than 0.

4. Experimental Results and Analysis

4.1. The Effect of HLS Translation

As everyone knows, the color space of a color image can be divided into R, G, B channels, which are equivalent to three gray images. The content of the original color image contained in the three channels is relatively average. If the secret information is embedded into any channel, the appearance of original color image may be greatly affected, and then the attacker’s suspicious will be aroused when it is transmitted in public channels. When a color image is covered into HLS channels, the H-channel image occupied most of the texture features of the original color image, so it is very suitable for embedding cover. Figure 3 shows the differences between RGB and HLS color spaces.

![Figure 3](image)

**Figure 3.** The difference between RGB and HLS color spaces. The left-most image is the original color image. The first row on the right represents the RGB three-channel images and the second row represents the HLS three-channel images. It is obvious that the H-channel image occupied most of the texture features of the original color image.

4.2. Security

Security is crucial to image steganography. To judge whether there is difference between two images, the most basic thing is that the human perception system will not detect the difference in the first place, then the basic histogram distribution of original image and steg image is analyzed, and figure 4 shows the specific experimental results.

In experiments, the embedding payload is setting to 0.4 bpp. The experimental results in figure 4 can reflect that no distortion occurred in the steg image due to the embedding of secret information. The histogram distribution is further analyzed. Although the payload is setting to 0.4 bpp, the histogram distribution does not change much, which indicates the security proposed in this paper is guaranteed.
4.3. Ability to Resist Steganalysis

The counterpart of image steganography is steganalysis technology, which detects whether secret information is embedded into a cover image. The specific process of steganalysis can be decomposed into two steps: feature extraction and classifier training. The purpose of classifier is to judge whether the secret information is embedded into the cover image, which is obviously a binary classification problem. Convolutional neural networks can learn the intrinsic features of high-dimensional data and has high recognition rate. Therefore, many researchers have introduced the technology of convolutional neural networks into the design requirements of steganalysis methods. The most popular methods of XuNet, YeNet are employed to detect the steg image embedded secret information. And the experimental results show that the detecting rate can be less than 60% when payload is 0.1 bpp. The ability to resist different steganalysis methods is shown in table 1.

| Payload (bpp) | Detecting Rate (%) |
|--------------|-------------------|
| 0.1          | 53.3%             |
| 0.2          | 61.3%             |
| 0.3          | 72.44%            |
| 0.4          | 81.9%             |

5. Conclusion

This paper proposed a novel steganography scheme for color image based on HLS translation. Firstly, the color cover image is divided from RGB channel into the HLS channel to obtain the three grayscale images. And the image of H channel has the most of texture features of original color cover image, so choosing the image of H channel has high security. Then the universal distortion function UNIWARD is utilized to embed the secret information into the cover image of H channel. This method proposed in this paper extends grayscale image steganography to color image, which makes the application of image steganography more extensive. At the same time, extensive experiments have shown that the scheme has high security and anti-steganalysis ability.

References

[1] Sedighi V, Cogranne R and Fridrich J 2015 Content-adaptive steganography by minimizing statistical detectability IEEE Transactions on Information Forensics and Security 11 (2) 221-234.
[2] Satir E and Hakan I 2012 A compression-based text steganography method *Journal of Systems and Software* **85** (10) 2385-2394.

[3] Li Q, Wang X, Wang X, et al. 2021 An encrypted coverless information hiding method based on generative models *Information Sciences* **553** 19-30.

[4] Fridrich J, Pevný T and Kodovský J 2007 Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities *Proceedings of the 9th ACM Multimedia & Security Workshop* pp 3-14.

[5] Fridrich J, Goljan M and Soukal D 2005 Perturbed quantization steganography *ACM Multimedia System Journal* **11** (2) 98-107.

[6] Filler T and Fridrich J 2010 Gibbs construction in steganography *IEEE Transactions on Information Forensics and Security* **5** (4) 705-720.

[7] Li Q, Wang X, Wang X, et al. 2020 A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks *IEEE Access* (99) 1-1.

[8] Holub V and Fridrich J 2012 Designing steganographic distortion using directional filters *IEEE Workshop on Information Forensic and Security, Tenerife, Canary Islands*.

[9] Holub V, Fridrich J and Denemark T 2014 Universal distortion function for steganography in an arbitrary domain *EURASIP Journal on Information Security, (Section: SI: Revised Selected Papers of ACM IH and MMS 2013)* pp 45-51.

[10] Fridrich J and Kodovsky J 2015 Rich models for steganalysis of digital images *IEEE Transactions on Information Forensics and Security* **9** (7) 321-332.

[11] Tan S and Li B 2014 Stacked convolutional auto-encoders for steganalysis of digital images *IEEE 2014 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)* pp 1-4.

[12] Qian Y, et al. 2015 Deep learning for steganalysis via convolutional neural networks *IS&T/SPIE Electronic Imaging* **9409** 94090J-94090J-10.

[13] Xu G S, Wu H Z and Shi Y Q 2016 Structural design of convolutional neural networks for steganalysis *IEEE Signal Processing Letters* **23** (5) 708-712.

[14] Jian Y, Ni J Q and Yi Y 2017 Deep learning hierarchical representations for image steganalysis *IEEE Transactions on Information Forensics and Security* **12** (11) 2545-2557.

[15] Li B, et al. 2018 ReST-Net: Diverse activation modules and parallel subnets-based CNN for spatial image steganalysis *IEEE Signal Processing Letters* **25** (5) 650-654.