Proposal Algorithm for Image Steganography by Hue Wavelet Transform Using Histogram

Maisa'a Abid Ali Kodher: Lecturer
Computer Sciences
University of Technology/Baghdad
Maisaa_ali2007@yahoo.com

Muntaha K. Abbas: Ass.Prof.
Technical College of Management/Baghdad
Middle Technical University
muntahaabbas@yahoo.com

Abstract

The rapid developments in communications systems and image transfer over the internet have led to the need for a new algorithm to hide text messages and images. The research presents dual method and 2-D wavelet transform method. In the first method, the colored image is transferred to Hue Saturation Lightness (HSL), while the second method, the Hue Saturation Lightness image is compressed by using 2-D wavelet transform (2DWT) to the L1, L2, and L3. After using the secret key to hide the compressed image the hidden image is produced. The secret key is a colored image from which statistical gradient of color image is taken and after the statistical gradient or histogram is obtained, it is possible to use cover image with a secret key to hide message under cover image.

The results that have been obtained in this proposed algorithm are based on the hidden image of capacity and robustness against attacks, and the generation of the secret key, which the original image can be retrieved without the recipient losing the data in the network.

Key word: Hue image, Image wavelet DWT, Secret key histogram, Steganography.

اقتراح خوارزمية أخفاء صورة بواسطة تحويل الموجة الثنائية باستخدام التدرج

ميساء عبد علي خضر:مدرس
قسم علوم الحاسوب
الجامعة التكنولوجية/ بغداد

منتهى خضير عباس:أستاذ مساعد
الكلية التقنية الادارية / بغداد
الجامعة التقنية الوسطى

المستخلص

ان التطورات السريعة في انظمة الاتصالات ونقل الصور عبر شبكة الانترنيت ادت الى ايجاد خوارزمية جديدة لاجل اخفاء رسالة نصية. ان هذا البحث يقدم طريقة مزدوجة تتكون من طريقة التدرج اللوني (Hue) وطريقة تحويل الموجة الثنائية الابعاد 2D.

في الطريقة الاولى يجري تحويل الصورة الملونة الى خفة اشباع لوني (Hue Saturation Lightness). وبعدها يتم ضغط صورة التدرج اللوني (Hue) وفي الطريقة الثانية يتم ضغط صورة خفة اشباع لوني بطريقة التحويل الموجة الثنائية الابعاد 2D الى المستوى L1 L3, L2, . وبعد استخدام المفتاح السري لاخفاء الصورة المضغوطة نحصل على صورة مخفية ، والمفتاح السري هو عبارة عن صورة ملونة ناخذ منها التدرج الاحصائي للصورة وبعد الحصول على التدرج الاحصائي ممكن استخدامه مع صورة الغطاء كمفتاح سري لاخفاء الرسالة تحت صورة الغطاء.

تعتمد النتائج التي تم الحصول عليها في هذه الخوارزمية المقترحة على الصورة المخفية ذات سعة وقوة ضد الهجوم. وتوليد المفتاح السري الذي يمكن عن طريقه استرجاع الصورة الاصلية دون ان يفقد المستلم البيانات في الشبكة.

1- Introduction

Steganography is the art of hiding information in an effort to conceal the existence of the embedded information [1].

Steganography is most often associated with the high-tech variety, where data is hidden within other data in any file. Combining the art of steganography with advanced robustness computers, networks, and the Internet has brought this method of hiding information to a new level [2]. Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years [3].

Information hiding is a general term encompassing many sub disciplines. One of the most important sub disciplines is Steganography Methods of Steganography have been mostly applied to image, audio, videos and text files while the major characteristics of these methods are to change in the structure and features so as not to be identifiable by human users [4].

2- Color Mode Hue Saturation Lightness Image

Hue is another word for color, ***Saturation*** (chroma) is the intensity or purity of a hue, ***Lightness*** (value) is the relative degree of black or white mixed with a given hue [5].

2.1- Hues are colors and what is hue dependent on the wavelength of light being reflected or produced can be seen. The Hue is adjustment command which will allow you to desaturate or change a color over an entire image or on a selected range of colors [6].

2.2- Saturation refers to how pure or intense a given hue is. 100% saturation means there is no addition of gray to the hue. The color is completely pure. At the other extreme a hue with 0% saturation appears as a medium gray. The more saturated (closer to 100%) a color is, the more vivid or brighter it appears. Desaturated colors, on the other hand, appear duller [5].

How saturated a hue appears also depends to a degree on what colors it's next to. A 50% saturated hue placed next to a 25% saturated hue will appear more vivid than were the same hue placed next to a 75% saturated hue.

2.3- Lightness measures the relative degree of black or white that has been mixed with a given hue. Adding white makes the color lighter (creates tints) and adding black makes it darker (creates shades). The effect of lightness or value is relative to other values in the composition. Lighter color can be made lighter by placing it next to a darker color [5].

3- Wavelet Transform Image Compression

Wavelets are special functions which are used as basic functions for representing signals. The discrete wavelet transform (DWT) has been applied here, the simplest DWT. In DWT the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels [7].

For 2-D images, applying DWT separates the image into a lower resolution approximation image or band (LL) and horizontal (HL), vertical (LH) and diagonal (HH) components as shown in figure (1) [7].

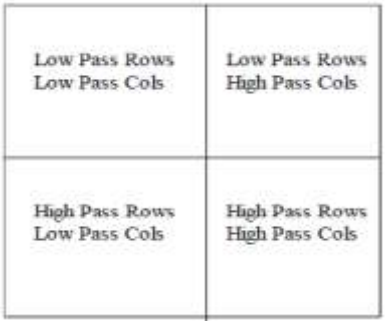


Figure (1) DWT Transform Image

4- Image Steganography Protocols

Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is sent to the receiver. On the other hand, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthorized persons can only notice the transmission of an image but can't guess the existence of the hidden message [8].

The most common approaches to information hiding in images are [9]:
1- Least significant bit (LSB) insertion.
2- Masking and filtering techniques.
3- Transformations (DCT, DWT).

5- Type of Steganography Protocols

There are mainly three types of steganographic protocols: pure steganography, secret key steganography, and public key steganography. In the following subsections, all three types will be discussed[10].

1. Pure Steganography: this type does not require the prior exchange of some secret information (such as a stego key). The embedding process can be described as a mapping :

$$\mathbf{E: C \times M \rightarrow C \ldots (1)}$$

where **C** is the set of possible covers and **M** the set of possible messages. The extraction process consists of a mapping:

$$\mathbf{D : C \rightarrow M \ldots (2)}$$

the secret message is extracted out of a cover. Clearly, it is necessary that $|\mathbf{C}| \geq |\mathbf{M}|$.

The embedding and extraction algorithms should not be public and both sender and receiver must have access to them.

2. Secret Key Steganography: is similar to a symmetric cipher, a cover C was chosen and the secret message was embedded into **C** using a secret key **k**. If the receiver knows the key used in the embedding process, he can reverse the process and extract the secret message. Generally, anybody who does not know the secret key should not be able to obtain the secret information. Formally, the embedding process is a mapping: [10]

$$E_k : C \times M \times K \rightarrow C \ldots (3)$$

and the extracting process is a mapping

$$D_k : C \times K \rightarrow M \ldots (4)$$

Where k is the set of all possible secret keys

3. Public Key Steganography: this type does not depend on the exchange of a secret key. It requires the use of two keys, one private and one public key; the public key is stored in a public database whereas the private key is used in the embedding process, the private key is used to reconstruct the secret message [10].

6- Proposed Algorithm

Step one:

The color image is converted from **RGB** to **HSL**, the type of image is **BMP** and size of image is **200×150** as shown in figure (2-a, b).

This step consider the cover for stego image to hide message under this cover.

Figure (2-a) Original Image

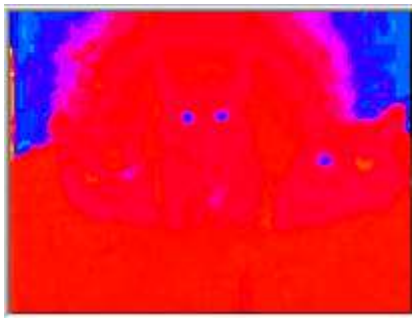


Figure (2-b) Hue of Image

Step two:

After image is converted to hue saturation Lightness it is in compression hue image in **2D** discrete wavelet it is Transform into three levels: First Level **L1**, Second Level **L2**, and third Level **L3**. The compressed image is obtained in L1 is **four parts**, in L2 is **sixteen parts**, and in L3 is **thirty two parts** and all levels are in small size for easy transmission across Internet Network the levels are shown in figure (3-a, b, c). And obtained the hue wavelet image transform, it called cover as shown in figure (4).

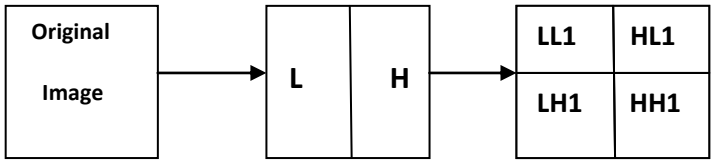
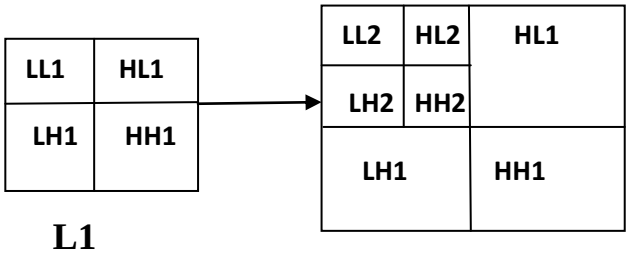


Figure (3-a) Decomposed First Level four parts



L1 **L2**

Figure (3-b) Decomposed Second Level sixteen parts

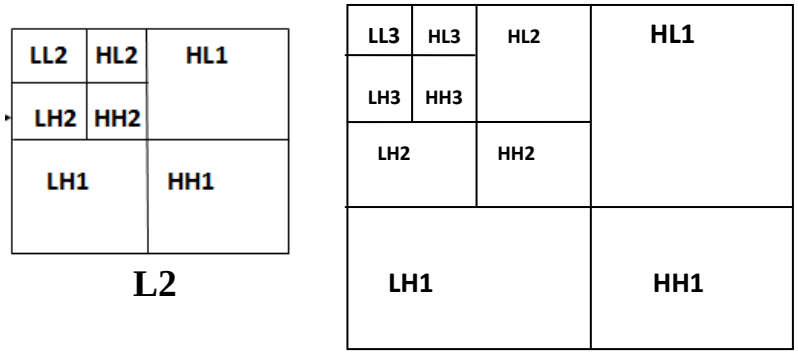


Figure (3-c) Decomposed Third Level thirty two parts

Figure (4) Hue wavelet image

Step three:

A secret key is generated by using gray-scale image; the size of image is **96×96** and type of image **BMP,** to calculate this image histogram. The calculation of the histogram takes the number of frequent values of pixel in image in axis Y but the axis X is the value of gray-scale in image from 0 to 255. After obtaining the figure of histogram it is considered a secret key as shown in figure (5).

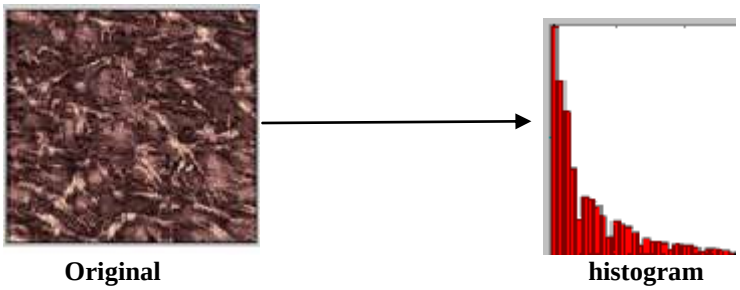


Figure (5) A secret key

Step four:

In this step the original image is transform to stego image using function of multiply hue wavelet image in L1, L2, and L3 (cover)

with a secret key generated, and after passing the function, it becomes the stego image in small size which is the same size as that of hue wavelet in L1, L2, and L3 as shown in figure (6-a, b).

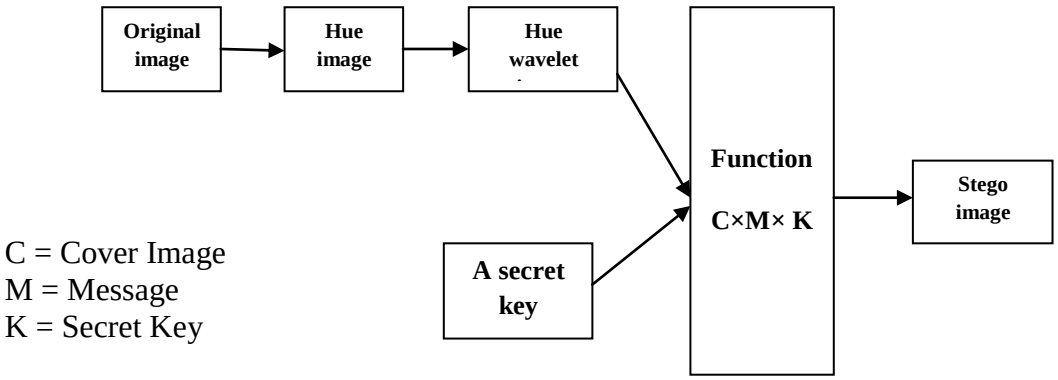


Figure (6-a)

Example:

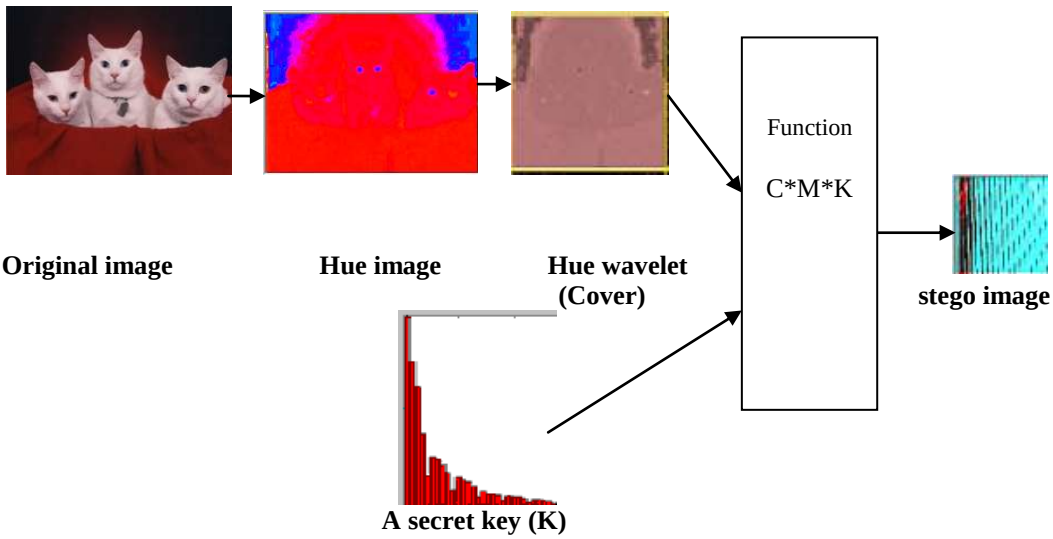


Figure (6-b) Transform of the original image to stego image

- The block diagram shown in figure (7) explains the main idea of the proposed embedding algorithm.

Start ➔RGB to Hue➔Hue compression➔ DWT (L1, L2, and L3) ➔ ➔Multiply histogram a secret key➔Stego-image.

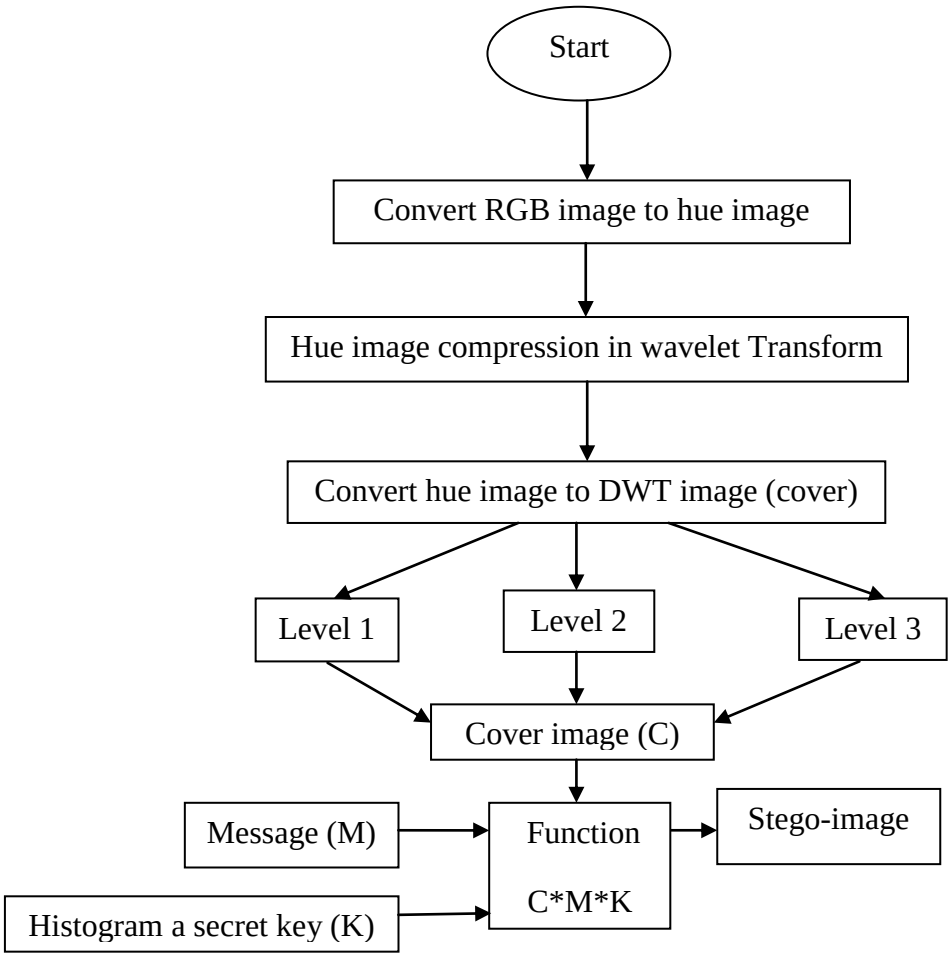


Figure (7) Block Diagram of the proposed Embedding Algorithm

6.1- Algorithm

In this algorithm the text, message, audio or video is embedded using cover image and a secret key histogram to obtain stego image to be sent from sender to receiver.

Process Algorithm:
Input: Original Image
Output: Stego-Image
Initial:
A : Load Original Image
B : Load Hue Image
C : Load Hue Wavelet Transform Image (cover Image)
D : Load Image Histogram (Secret Key)
E : Stego-Image
Step 1: Convert the original image RGB to Hue saturation Lightness in B.
Step 2: Find cover image from hue image to compression DWT in C.
Step 3: Select three levels to compression image in L1, L2, and L3.
Step 4: Compression image hue wavelet in first level (L1) in C.
Step 5: Compression image hue wavelet in second level (L2) in C.
Step 6: Compression image hue wavelet in third level (L3) in C.
Step 7: Find a secret key from color image to convert to histogram in D.
Step 8: Multiply cover image hue wavelet in L1, L2, and L3 with secret key in D.
Step 9: Result (Put the result Stego-Image in E).

6.2- Test of Result

In this test three examples in three levels are used to transform images hue wavelet to stego image, as shown in tables (1, 2,and 3).

The robustness of stego image is examined peak single noise ratio (PSNR) and correlation as shown in tables shown in table (4).

Table (1)

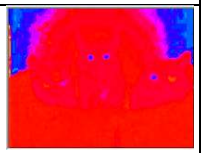
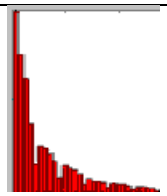
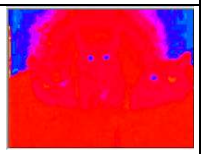
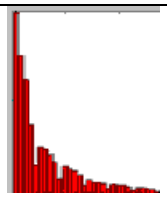
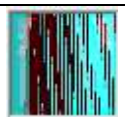
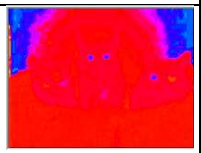
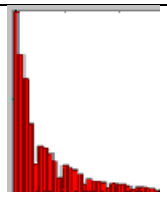
Original image cat	Hue image	No. of level	Hue wavelet	Secret key	Stego-image
		L1			
		L2			
		L3			

Table (2)

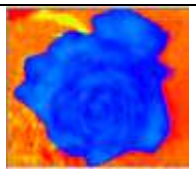
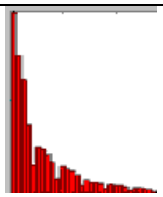
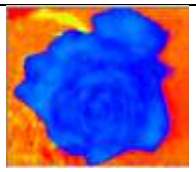
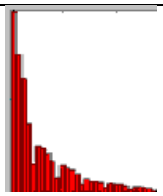
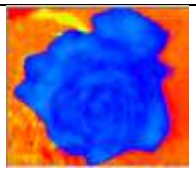
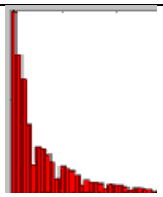
Original image flower	Hue image	No. of level	Hue wavelet	Secret key	Stego-image
		L1			
		L2			
		L3			

Table (3)

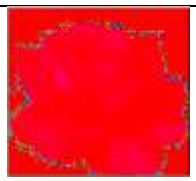
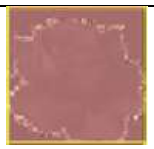
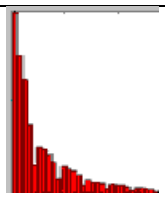
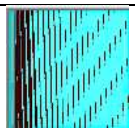
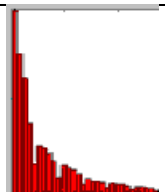
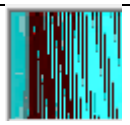
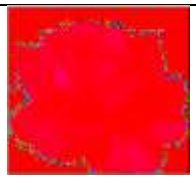
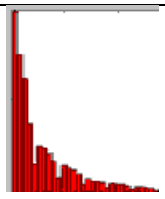
Original image rose	Hue image	No. of level	Hue wavelet	Secret key	Stego-image
		L1			
		L2			
		L3			

Table (4)

Name original image	No of level	PSNR	Correlation measure
Cat	L1	0.9409	2621.9012
Cat	L2	0.8739	2590.3677
Cat	L3	0.4256	2546.3210
Flower	L1	0.8383	2610.7738
Flower	L2	0.6641	2597.o188
Flower	L3	0.3513	2568.6441
Rose	L1	0.8126	2645.7882
Rose	L2	0.7590	2602.8028
Rose	L3	0.4089	2504.9703

7- Conclusions

This paper provides a good and efficient method for image steganography by reducing image size for transmitting to the destination across network and internet in a secure way.

In this system, the image data is converted to hue saturation lightness. The system transforms the image to hue wavelet in three levels, L1, L2, and L3. Which consist of 4, 16, and 32 parts respectively, the compressed image takes small size and is more robust in a secure way.

The image becomes a suitable cover for small size and conceals message without detection.

The stego image is examined by using PSNR and correlation, as shown in table (4). The stego image values vary with hue wavelet transform, thus increasing the conceal image efficiency.

The values of PSNR range in all examination from 0.9 to 0.4 in all levels, and the values of correlation range in all examination from 2621.90 to 2504.97 in all levels.

These values give more robustness against attacks and protect stego image, this means the algorithm is efficient during the transmission.

8- References

1- Arvind Kumar, Km. Pooja, " Steganography- A Data Hiding Technique", International Journal of Computer Applications, (0975– 8887) Vol.9, No.7, November 2010.

2- Eric Cole , Ronald D. Krutz," Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley publishing, In.2003.

3- James C.," Steganography: Past, Present, Future". SANS Institute Publication, 2001.
Available at:
http://www.sans.org/reading_room/whitepapers/stenganography/stegan-ographypastpresent-future_552.

4- Rajesh Shah, Yashwant Singh Chouhan, " Encoding of Hindi Text Using Steganography Technique", International Journal of Scientific Research in Computer Science and Engineering, Vol.2, Issue-1, 2014.

5- "The Fundamentals of Color: Hue, Saturation, And Lightness". Available at:
http://www.vanseodesign.com/web-design/hue-saturation-and-lightness/

6- " Fix Out-of-Gamut Images - Hue and Saturation".
Available at:
http://www.udel.edu/cookbook/class/Tricks/fixgamut-uesat.pdf

7- Gurmeet Kaur , Aarti Kochhar, "Transform Domain Analysis of Image Steganography ", International Journal for Science and Emerging Technologies with Latest Trends" 6(1): 29-37, 2013.

8- Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 3 No. 9 Sep 2012.

9- Sabu M Thampi, "Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

10- Sattar B, Abbas M, Naween N.," An Agent based Image Steganography using Information Theoretic Parameters", MASAUM Journal of Computing, 1(2): 258-264, 2009.