

# Steganography with Digital Image Technique On Integer Wavelet Transform Cielab

R M Alhaziyah<sup>1</sup>, U Rizal<sup>2</sup>

<sup>1</sup> Studies Program Information System, Faculty of Computer Science, Bandar Lampung University, e-mail : miaalhaziyahratu@gmail.com

<sup>2</sup> Faculty of Computer Science, University of Bandar Lampung, Indonesia, e-mail : usman.rizal@ubl.ac.id

**Abstract.** Remarkable progress in the field of information technology and telecommunications led to the emergence of demand for secure communication environment and have privacy. Steganography is a method used to disguise the presence of confidential information, making it difficult to detect its presence by people who do not have the authority for the information. Additionally, steganography can be applied to multimedia such as text, images, audio / video and protocols. Problems often arise in research on steganography, among others, the low capacity of concealment, less pharmaceuticals stego-image, as well as the poor quality of stego-image is generated. This study aims to create a digital image steganography safe, sturdy, has a high masking capacity and has good imperceptibility, so the fidelity and recovery capabilities will be good anyway. The method proposed in this study manggabungkan Integer Wavelet Transform technique that aims to increase the capacity of concealment Furthermore this research is done on the CIELAB color space, where CIELAB can produce digital images with high compression range and a small color deviations on wavelet transform. In the watermarking technique in wavelet domain, CIELAB has the most excellent robustness compared with other color spaces. For security measures, used steganalyzer's ROC performance and PSNR of the quality of stego-image is generated. Keywords. *Steganography, Integer Wavelet Transform, CIELAB colorspace*

## 1. Introduction

Tremendous development of information and communication technologies have increased the demand for secure communication environment and have privacy. Classic problem regarding covert communication was first presented by the Simons known as the prisoner's problem contained on where Bob and Alice are prisoners who are placed in separate cells, they can communicate through the intermediary of a warden named Wendy. Such conditions they may not encrypt the message contains an escape plan that they convey through Wendy guards, because it will certainly lead to the suspicion of the warden. How can Bob send a secret message to Alice without being suspected by the warden Wendy? Steganography is the solution.



Figure 1. The problem of Prisoners (Prisoner's Problem)

## 2. Theoretical

Steganography is a technique of hiding the existence of information on digital media in a media that does not have hidden or suspicious information called Media stego / media cover, where

Steganography can meet the interests of both legal and illegal. Speaking steganography means talking about information hiding technique. Some data hiding techniques be developed for the purpose of preventing the theft of data, control the number of copies of documents, e-commerce, electronic transactions protection, secret communications, and so on. Some of the concealment techniques commonly known information:

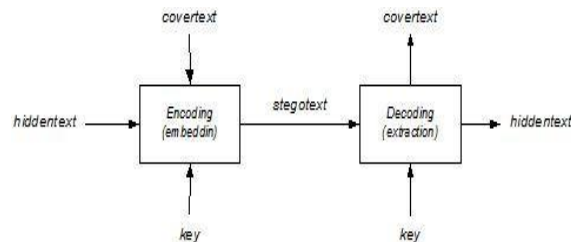
- a. Cryptography: hide the content (content) messages with the aim that the message can not be read by people who do not have the authority.
- b. Digital Watermarking: providing a watermark (watermark) on the original document aims to prevent copyright infringement.
- c. Steganography : hiding the existence (existence) message, aiming to avoid suspicion (conspicuous)

**Table 1.**Information Hiding Technique

Teknik Penyembunyian Informasi		
Kriptografi	Digital Watermarking	Steganografi

Steganography comes from the Greek word, 'Steganos' and 'graphein', which means hidden writing (writing covered). Steganography is also defined as the art of hiding communication by embedding secret message into the document cover, such as digital images, for example. Steganography is the art of hiding the fact when communication takes place, by hiding information in other so that no one apart from the intended recipient knows of the existence of the message. It is the art of hiding messages in an envelope and without leaving a trace on the original message.

Steganography history begins with the head slave media (narrated by Herodatus, the ruler of Greece in 440 BC in the book: Histories of Herodatus). Histaeus slave head dibotaki, ditattoo a message, the slave hair is allowed to grow, slaves shipped. In place of the slave head shaved recipients for a message to be read.



**Figure 2.** Model Steganography

Properties on steganography namely:

- A. Embedded message (hiddentext): that is the message that is hidden, it can be in the form of text, images, audio, video or protocol.
- B. Cover-object (cover medium): that is the message that is used to hide the embedded message, can be text, images, audio, video or protocol.
- C. Stego-object (stego medium): image / object that already contains an embedded message.
- D. Stego-key: the key that is used to insert and extract messages from the message stego medium.

Three criteria in assessing the performance of steganographic techniques, namely:

- A. Security, where steganography should be safe from a variety of active and passive attacks. If the existence of a secret message can not be estimated with a higher probability of a random guesses steganalysis some systems, it can be said safely steganography. For security measure can be used steganalyzer's ROC performance that serves to identify the presence or absence of media that allegedly embedded secret data.
- B. Capacity, which is so useful to convey secret messages, capacity hidden provided by steganography should be as high as possible, which can be given in absolute measurement (such as the size of the secret message), or a relative value (called the insertion rate of data, such as bits per pixel, bits per non-zero discrete cosine transform coefficient, or the ratio of a secret message to the media cover).

C. Imperceptibility, namely the existence of a secret message can not be perceived by the human senses. Related to imperceptibility here is fidelity, quality of steganography media after the insertion process the message should not change significantly, as well as the recovery, the message must be extracted whenever needed. Steganography can be implemented in almost all types of multimedia files (text, images, audio and video), but the most commonly used is the digital image, because the exchange of data in the form of digital images on the Internet is quite high, so that it can reduce the level of suspicion of a hidden message which has been inserted.

Problems often arise in research on steganography, among others, the low capacity of concealment, less robust and low quality of stego-image is generated. Two schemes commonly used to create a digital image steganography has advantages and disadvantages of each. Mechanical insertion in the spatial domain, for example, is a technique Least Significant Bit (LSB) substitution, have excess capacity high concealment and easy to control the quality of the stego-image, but weak in robustness and also has a low imperceptibility. Another scheme is the domain transform technique which can cover weaknesses that exist in the spatial domain insertion technique. One technique that is frequently used domain transform is discrete cosine transform (DCT), which is commonly used in the compression of JPEG images and MPEG. There is also a discrete wavelet transform and discrete Fourier transform which is widely used in the current research were applied to the compression of images with the JPEG 2000 format and MPEG4. Excess techniques transform domain of spatial domain techniques is their ability to tolerate high enough noise signal process several operations. However, they also have the disadvantage of a high computational complexity that resulted in them being slower and lower hiding capacity.

### 2.1 Integer Wavelet Transform

Generally domain wavelet allows us to hide data in areas that are less sensitive to the human visual system (HVS), such as ribbons detailed high resolution (HL, LH and HH), hiding data in this area allows us to increase the robustness (robustness) while maintaining excellent visual quality. Integer integer wavelet transform map data set to another integer data sets. In the Discrete Wavelet Transform (DWT), filter wavelet used has a coefficient of floating point numbers so that when we hide data within that coefficient, some cuts of floating point values of the pixels must be integers can cause loss of hidden information that can lead to failure of the steganographic system. To avoid the problem of floating point precision of the filter wavelet when the input data are integers such as digital images, the data output will no longer be an integer that does not allow the reconstruction perfect from the input image and in this case there will be no information is lost through the modifier forward (forward transform) and inverse converter (inverse transform). Because mentioned the difference between wavelet transform integers (IWT) and wavelet transform discrete (DWT), sub-band LL in the case of IWT appears to be a copy of which is very similar to the smaller scale of the original image, while in the case of DWT sub-band LL resulting distorted. Lifting scheme is one of many techniques that can be used to perform integer wavelet transformation scheme is also used in this study. Here's an example that shows how we can use to get the lifting scheme wavelet transform decimal integer by using simple cutting and without losing something that can not be avoided.

Hair wavelet transform can be written as the average pairwise simple and differences

$$\begin{aligned} S_{1, n} &= (S_{0.2n} + S_{0.2}) / 2 \\ d_{1, n} &= S_{0.2n} - S_{0.2} \end{aligned} \quad (1)$$

where  $S_{i, 1}$  in, 1 is the  $n$ th low frequency and high frequency wavelet coefficients at the level of the respectively. It is clear that the output is not an integer, the Hair wavelet transform in (1) can be rewritten using lifting in two steps to be performed sequentially:

$$\begin{aligned} d_{1, n} &= S_{0.2n+1} - S_{0.2n} \\ S_{1, n} &= S_{0.2n} + d_{1, n} / 2 \end{aligned} \quad (2)$$

From (1) and (2) we can calculate the integer wavelet transform becomes:

$$\begin{aligned} d_{1, n} &= S_{0.2n+1} - S_{0.2n} \\ S_{1, n} &= 0.2n + (d_{1, n} / 2) \end{aligned} \quad (3)$$

Then inverse transformation can be calculated with

$$S0.2, n = SI.n - (d1, n / 2)$$

$$S0.2n + 1 = dl, n + S0.2, n \quad (4)$$

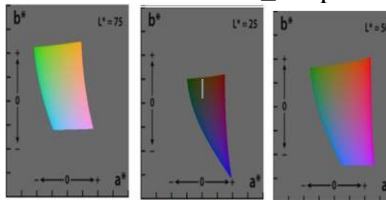
Usually wavelet transform research with this technique performed on the RGB color space. But in this study, the wavelet transform performed on the CIELAB color space, where CIELAB can produce digital images with high compression range and a small color deviations on wavelet transform. In the watermarking technique in wavelet domain, CIELAB has the most excellent robustness compared with other color spaces.

### 2.2 CIE 1976 L \* a \* b \*

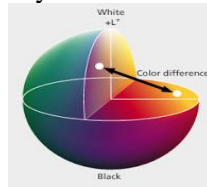
CIELAB is defined CIE color space also in 1976 (CIE 1976 L \* a \* b \*) is the formula of a second after CIELUV; second CIELUV and CIELAB color space conversion function that has an 1: 1, so the color space is identical, only the appearance of different besaaran.

With CIELAB we started on the view and the meaning of each dimension is formed, namely:

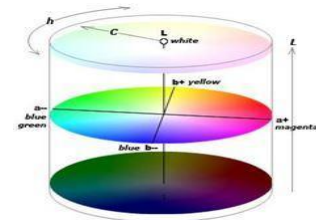
- Magnitude CIE\_L \* to describe the brightness of the color, 0 for black and L \* = 100 for white),
- Dimensions CIE\_a \* describes the type of green color - red, where the numbers negative a \* indicates the green and vice versa CIE\_a \* positive indicates red,
- Dimensions CIE\_b \* for the kind of blue color - yellow, where negative numbers b \* indicates blue and vice versa CIE\_b \* positive indicates yellow.



**Figure 3.** CIEL \* a \* b \* Color Model



**Figure 4.** CIEL \* a \* b \* color 3D model



**Figure 5.** Diagram chromaticity a \* b \*

### 2.3 Chromaticity a \* b \*

Because CIELAB is also a three-dimensional model, the CIELAB only be described correctly when the three-dimensional space, and if we take slices of components a \* and b \* , then we will get a chromaticity diagram a \* b \*. Chromaticity diagram a \* b \* below to further explain the broad chromaticity a \* b \* at a brightness level (CIE\_L \*) certain, namely CIE\_L \* = 75, CIE\_L \* = 50 and CIE\_L \* = 25. At maximum brightness level CIE\_L \* and CIE\_L minimum \* = 0 field chromaticity a \* b \* becomes small close to 0, so simply we can imagine that the CIELAB color model such as a spherical shape. The neutral point there is positioned CIE\_b CIE\_a \* = \* = 0 (achromatic line) Note that the color space is a derivative of the color space "seed" CIEXYZ that have long been defined by the CIE own. The room is the most popular colors used in the field of Color Management System in the graphics industry. CIELAB also has a cylindrical model which CIELChab which has almost the same meaning CIELChuv.

CIEL \* a \* b \* (CIELAB) is the most complete color space. This color space describes all colors that can be seen by the human eye and is made such that it is independent does not depend on the tools and processes, so that the ICC - International Color Consortium using color space CIEXYZ and CIELAB as the basis for calculation of color communication (PCS - Profile Communication Space) in color Management System, and CIELAB used to describe the color, the color difference and tolerance in the international standard ISO 12647. This study aims to assess the use of techniques Integer Wavelet Transform algorithms using Pixel Optimum adjustment in a color space CIELAB to obtain digital image steganography safe, sturdy, has a high masking capacity and has good imperceptibility, so the fidelity and recovery capabilities will be good anyway, take measurements of steganalyzer's security by using ROC performance and the measure PSNR to know imperceptibility, fidelity and recovery of stego-image is generated.

### 3. Research Methodology

#### 3.1 Proposed Research Methods

In this research method is proposed to create a model of Digital Image Steganography Techniques Using Integer Wavelet Transform In CIELAB Color Space.

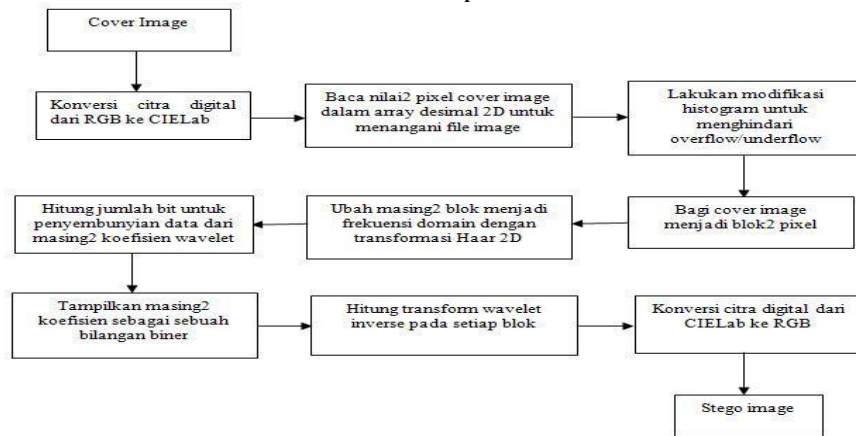


Figure 6 Embedding Process

#### 3.1.1 Insertion Algorithm

Block on insertion algorithm described in the following steps:

Step 1 :

Converting the digital image from RGB to color space CIELAB with the following formulation:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.412 & 0.358 & 0.180 \\ 0.213 & 0.715 & 0.072 \\ 0.019 & 0.119 & 0.950 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

$$L^* = \begin{cases} 116(Y/Y_n)^{1/3} - 16 & (Y/Y_n) > 0.008856 \\ 903(Y/Y_n)^{1/3} & (Y/Y_n) \leq 0.008856 \end{cases} \quad (2)$$

$$\begin{cases} a^* = 500[f(X/X_n) - f(Y/Y_n)] \\ b^* = 200[f(Y/Y_n) - f(Z/Z_n)] \end{cases} \quad (3)$$

$$f(q) = \begin{cases} q^{1/3} & (q > 0.008856) \\ 7.787q + 16/116 & (q \leq 0.008856) \end{cases} \quad (4)$$

dimana  $X_n = 95.047$ ,  $Y_n = 100$ ,  $Z_n = 108.883$

Step 2:

Read the pixel value of the cover image in an array of decimal 2D to more easily handle the image file.

Step 3:

Make modifications to the histogram to prevent overflow / underflow when the value converted into integer wavelet coefficients that produce the stego-image pixel value exceeds the value of 255 or less than 0. the newly discovered problems are caused by values close to 255 or 0.

Step 4:

For the cover image into 8x8 blocks that do not overlap. With this division, each 8x8 block can be categorized as a block of complex.

Step 5:

Change each block into a transform domain using wavelet transform integer Hair 2D generate LLI, LHI, HLI and HHI.

Step 6:

Calculate the number of bits for concealment Data from wavelet coefficients masing2.

Step 7:

Insert bit L of the message into coefficients which have been selected at random. Random selection of coefficients made safer where the sequence of messages known only to the sender and receiver using a secret key that has been approved.

Step 8:

Apply Pixel Adjustment Optimum algorithms. The main idea is to use this algoritma perbedaan minimize the error between the original coefficient values with values transformed by checking bit to the right to modify the altered LSB so that the results will be minimal. This algorithm is the final step of the proposed scheme, in which the algorithm is to minimize errors up to half.

Step 9:

Calculate the inverse integer wavelet transform on each block of 8x8 to save the image into the spatial domain.

Step 10:

$$X = X_n * (P + a^* / 500)^3 \quad (9)$$

$$Y = Y_n * P^3 \quad (10)$$

$$Z = Z_n * (P - b^* / 200)^3 \quad (11)$$

dimana  $P = (L^* + 16) / 116$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 3.240 & -1.537 & -0.498 \\ -0.969 & 1.875 & 0.041 \\ 0.055 & -0.204 & 1.057 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \quad (12)$$

### 3.1.2 Algorithm Extraction

Convert a digital image of the results of the previous steps of the CIELAB to RGB color space with the following formulation:

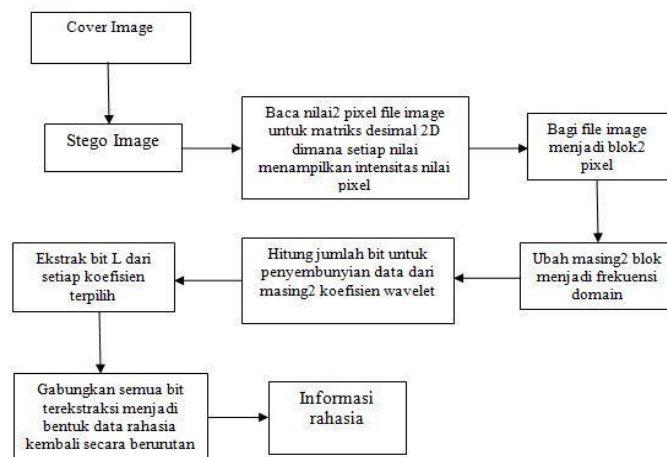





Figure 7 Extraction Process

## 4. Discussion

### 4.1 Analysis And Testing

Test images used in the experiment is sized 500x500 pixel shown in Table 2.

Table 2 Standard Test Used Citra

No	Citra asli	
1		Peta Pulau Sumatera.bmp (732 kb)
2		Kain.bmp (732 kb)
3		Bunga.bmp (761 kb)

Media placeholders for this experiment is the .bmp image files. While the message that will be inserted in this experiment is a text that can be input or can be typed directly in the text box steganography applications.

#### 4.2 Embedding Process Results

Image results Stego image message insertion (Map Sumatra.bmp Island) has a value of PSNR = 3.2 dB. PSNR (peak signal to noise ratio) is calculated by the formula MSE stands for Mean Squared Error.



**Figure 8.** Stego

#### 4.3 Ekstracting process results

Generally the extraction process messages in this experiment can be done well, besides the extraction of a message from the stego image generated in this experiment is complete exactly the same as the message file before the insertion process is done. The following explanation of the experiment in Table.

**Table 3** Results Ekstracting

Cover Image	PSNR(dB)	Ekstraksi
Peta Pulau Sumatera.bmp	3,2	Berhasil
Kain.bmp	4,1	Berhasil
Bunga.bmp	3,7	Berhasil

## 5. Conclusions and Recommendations

### 5.1 Conclusions

A proposed method of steganography digital image in the frequency domain was presented. The results of this experiment showed that the color space CIELAB can be used in steganography using Integer Wavelet Transform and can produce a stego-image with imperceptibility and fidelity is good enough based on the measurement results PSNR is still above 30 dB and stego-image the same exactly with the original image, in addition to the recovery rate of the stego-image messages generated very good because the message is inserted can be extracted intact as before.

### 5.2 Suggestions

Some suggestions for development, among others:

- A. Expected future researchers suggest there are other new research on steganography in the CIELAB color space, as there is currently a lot of research CIELAB color space is applied to steganography.
- B. For further development can be tested with image editing stego ie brightness, contrast, and cropping.
- C. Digital image that is used only image with .bmp format only for its further development could use the image formats such as .JPEG, .PNG, .TIFF, and .GIF.
- D. The study may be followed by other media such as audio and video.
- E. Steganography application is still being developed for a desktop computer device. It would be more practical if the hardware is developed for mobile phones.

### References

- [1] Hamsah A. Ghaleb Al-Jbara, Laiha Binti Mat Kiah, Hamid A. Jalab, *Increased Capacity of Image Based Steganography Using Artificial Neural Network*, Proc. International Conference on Fundamental and Applied Sciences in 2012.
- [2] GJ Simmons. *The Prisoner's Problem and the Subliminal Channel*, Proc. From CRYPTO'83, pp. 51-67, 1983.
- [3] Bin Li, Junhui He, Jiwu and Yun Qing Shi Huang, *A Survey on Image Steganography and steganalysis*, Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, 2011.
- [4] Farhan Khan Muhammad Rafat and Sher, Survey Report - *State Of The Art In Digital Steganography Focusing Ascii Text Documents*, (IJCSIS) International Journal of Computer Science and Information Security, **Vol. 7**, No. 2, 2010
- [5] Jessica Fridrich and Miroslav Goljan, *Practical steganalysis of Digital Images - State of the Art*, Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV, 2002
- [6] Emmy Poentarie, *Communication Strategy Implementation In PLIKs Nanggulan 2*, Journal of Communication and Media Studies, Hal: 163-172, **Vol. 17** No. 2, 2013
- [7] Adnan Mohsin Abdulazeez Brifcani and Wafaa Mustafa Abdulllah Brifcani, *Stego-Crypto-Based Technique for HighSecurity Applications*, International Journal of Computer Theory and Engineering, **Vol.2**, No.6, 2010.
- [8] Sharma and D. Sharmas, *Research on Analysis of Different Image Steganography Techniques*, International Journal of Engineering Sciences & Research Technology, 2014
- [9] Abdul Gabbar TA and Abdulmalek Abduljabbar A., *Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm*, (IJCSIS) International Journal of Computer Science and Information Security, **Vol. 13**, No. 1, 2015.
- [10] M. Wu, E. Tang, and B. Lin, *hiding data in digital binary image*, Proc. of 2000 IEEE International Conference on Multimedia and Expo, **vol. 1**, pp. 393-396, 2000.
- [11] Liang, S. Wang, and X. Zhang, *Steganography in binary image by checking the data-carrying eligibility of boundary pixels*, Journal of Shanghai University, **vol. 11**, no. 3, pp. 272-277, 2007.
- [12] Cayre and B. Macq, *hiding data on 3-D triangle meshes*, IEEE Trans. Signal Processing, **vol. 51**, no. 4, pp. 939-949, 2003.
- [13] Jessica Fridrich, Miroslav Goljan, and Rui Du, *Reliable detection of lsb andgrayscale*



- steganography in color images*. Proc. of 2001 ACM Workshop on Multimedia and security: new challenges, pp.27-30, ACM Press, 2001.
- [14] W. Bender, D. Gruhl, Morimoto N., and A. Lu, *Techniques for the data hiding*, IBM Systems Journal, **vol. 35**, no. 3, pp. 313-336, 1996.
- [15] Eiji Kawaguchi and Richard O. Eason, *Principle and applications of BPCS steganography*, In *Multimedia Systems and Applications*, **vol. 3528**, pp. 464-473, SPIE, 1998.
- [16] Zacharias, A and Munir, R, *Steganography digital image using Discrete Wavelet Transform technique on the CIELAB color space*, proceedings KNSI-ISSN: 1906-9613, 2015.
- [18] Jayasudha, S., *Integer Wavelet Transform Based Method Steganographic using OPA algorithm*, the International Journal of Engineering and Science-ISSN: 2278-4721, Vol. 2, pp. 31-35, 2013.
- [19] Roy, R., Changder, S., Sarkar, A., Debnath, *NC Evaluating image steganography techniques: Future research challenges*, IEEE Conference on Computing, Management and Telecommunications, 309-314, 2013.
- [20] Harmsen, J. and Pearlman, W.: *Statistical highorder of Palette Images*, in Proc. SPIE Security Watermarking of Multimedia Contents, 5020, 131-142., 2003.
- [21] Hemalatha, S., Acharya, UD, Renuka, A.: *Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB YCbCr And Domains*, International Journal of Advanced Information Technology, 3, 1-9. 2013.
- [22] Khalili, M. and D. Asatryan: *Color Spaces Effects on Improved Discrete Wavelet Transform-Based Digital Image Watermarking using Arnold Transform Map*, IET Signal Processing, 7, 177 - 187, 2013.
- [23] Mandal, JK and Das, D.: *Color Image Steganography Based on Pixel Value differencing in Spatial Domain*, International Journal of Information Sciences and Technique, 2, 83 - 93, 2012.
- [24] Hamid, N., Yahya, A. Ahmad, RB, Alqershi, OM, *Image Steganography Technique: an overview*, International Journal of Computer Science and Security (IJCSS), **Vol. 6**. Pp. 168-187, 2012.
- [25] János Schanda, COLORIMETRY - *Chapter 9 of the book OSA / AIP Handbook of Applied Photometry* (ed .: Dr. Casimer DeCusatis IBM, Poughkeepsie, NY US