Middle-East Journal of Scientific Research 22 (5): 647-654, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.22.05.21946

# A Novel Image Steganographic Approach for Hiding Text in Color Images Using HSI Color Model

[1]Khan Muhammad, [1]Jamil Ahmad, [2]Haleem Farman and [1]Muhammad Zubair

[1]Department of Computer Science, Islamia College Peshawar, Pakistan
[2]Department of Computer Science, University of Peshawar, Pakistan

**Abstract:** Image Steganography is the process of embedding text in images such that its existence cannot be detected by Human Visual System (HVS) and is known only to sender and receiver. This paper presents a novel approach for image steganography using Hue-Saturation-Intensity (HSI) color space based on Least Significant Bit (LSB). The proposed method transforms the image from RGB color space to Hue-Saturation-Intensity (HSI) color space and then embeds secret data inside the Intensity Plane (I-Plane) and transforms it back to RGB color model after embedding. The said technique is evaluated by both subjective and Objective Analysis. Experimentally it is found that the proposed method have larger Peak Signal-to Noise Ratio (PSNR) values, good imperceptibility and multiple security levels which shows its superiority as compared to several existing methods.

**Key words:** Image Steganography · HSI color model · Objective analysis · LSB · PSNR · Information Security

## INTRODUCTION

The word steganography is derived from two Greek words; "stegano" meaning protected and "graphia" meaning writing. It can be defined as the process of writing messages in a way in which the presence of secret message is known only to sender and receiver. Steganography require a carrier object, secret data and embedding algorithm. It may also need an encryption algorithm and secret key in some cases in order to increase the security levels of steganography. Applications of steganography includes secure transmission of top secret documents between national and international governments, securing online banking and voting systems, secret communication between criminals and terrorists and sending Trojan horses and viruses to attack on systems etc [1-7].

**Steganography VS Cryptography:** Steganography and Cryptography both techniques are used for data confidentiality (protection of information from unwanted parties).However there also exists some differences between them that is described below.

- Cryptography is the practice and study of secure communication but Steganography is an art as well as a science of covert communication.
- The main focus of Cryptography is to keep the contents of the data secret while Steganography aims to keep the existence of the data secret.
- To break the cryptography, we compare some sections of the plaintext with the sections of the cipher text but in breaking steganography we compare the cover object with the stego object plus some possible sections of the message.
- Cryptography fails when an intruder gain access to the contents of the cipher material but steganography fails only when a malicious user detects the presence of the secret data. The Table 1 given below also clarifies the difference between these techniques [8-10].

**Types of Steganography W.r.t Carrier Object:** Steganography embeds secret data into digital carriers like image, audio, video etc such that it cannot be easily detected by the Human Visual System (HVS). There are five types of steganography on the basis of carrier object

**Corresponding Author:** Khan Muhammad, Department of Computer Science, Islamia College Peshawar, Pakistan.

Table 1: Comparisons of Cryptography and Steganography

| | Comparison Table | | |
|---|---|---|---|
| Method/Property | Confidentiality | Integrity | Unremovability |
| Cryptography | Yes | No | Yes |
| Steganography | Yes/No | Yes/No | Yes |

Note: None of the above methods alone can be perfect and compromised.

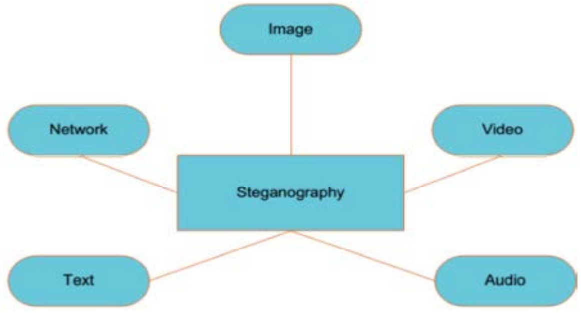

Fig. 1: Types of Steganography w.r.t carrier object

that is used for embedding the secret data. These types are briefly described and its diagrammatic representation is given in Fig. 1.

**Image Steganography:** The type of Steganography in which image is used as cover object is called Image Steganography. Generally, the techniques in this method modify the image pixels for hiding secret information. Images are considered to be the best cover objects/carriers for hiding information because it contains large amount of redundant bits.

**Network Steganography:** The type of Steganography in which network protocol (TCP, IP, UDP and ICMP etc) is used as cover object is called Network Steganography. In this method, information is hidden in some fields of the Header of TCP/IP packet that are optional or never used.

**Text Steganography:** Text Steganography uses text as a carrier for hiding secret information. In this technique secret message is hidden in the $n^{th}$ letter of every word of carrier text. Unlike other types of steganography (audio, video, network and image), Text steganography is much more difficult because of less redundancy in the text. Text steganography is preferable for simple communication where less memory is needed.

**Audio Steganography:** The type of steganography in which audio is used for encoding and decoding of secret data is called audio steganography. This type of steganography is considered as a significant medium for secret communication due to attractiveness of voice IP (VOIP). The different types of audio formats used for audio steganography are MPEG, MIDI, WAVE, AVI, etc.

**Video Steganography:** When video is used as a carrier for information hiding, then the steganography used is called video steganography. This approach is capable to hide large volume of data as video is the combination of frames/images and contains large amount of redundant bits. The formats used by video steganography are H.264, Mp4, MPEG, AVI etc.

This paper proposes a novel method for steganography to overcome the limitations of existing steganographic methods. Image has been chosen as a carrier object in this paper because it contains more redundant bits. The rest of the paper is organized as follows. Section 2 critically discusses some existing steganographic methods in literature whose defects led us towards current proposed work. The proposed technique is detailed in section 3. Section 4 is devoted to experimental results and discussion. The conclusion of the paper is given at the end in section 5.

**Literature Review:** The simplest method to hide secret data inside a cover image is LSB. In this method the least significant bits of the carrier image pixels are replaced with the secret data bits. Payload capacity of LSB method can be increased if more than 1 LSBs are used for message embedding but it brings noticeable changes in the carrier image. LSB method is simple to implement but it is vulnerable to many statistical attacks like RS, image processing operations and Chi-Square analysis etc. [11-17].

Adnan Abdul-Aziz Gutub proposed a more robust steganographic technique in [18] in which one channel is used for indication while other two channels are used for embedding secret data in a predefined cycle manner which enhances the robustness of proposed method. The experimental results show us the high payload capacity and better imperceptibility of the proposed algorithm. This method also avoids the key exchange overhead.

In [19], the authors propose a robust method which embeds variable bits in image pixels depending on the pixel value and value of mean and standard deviation (SD). Two bits are inserted in the image pixel if (mean–SD/2) is greater than pixel value; 3 bits are stored if (mean +SD/2) is greater than pixel value otherwise 4 bits are stored in each pixel value. Chaotic effect is also obtained in the proposed method by using random traversing path which make the attack loathsome but nothing is given about generating the random traversing path.

Grover *et al.* in [20], presents an adaptive edge based LSB substitution technique which hides three (3) bits of secret data in edgy pixel and two(2) secret bits in non-edgy pixels in blue channel of the RGB image. This method has high payload capacity and is more robust as compared to simple LSB substation method because secret data is divided into two sets first and then it is embedded in cover image starting from the central pixel and traversing through the whole image which increases its robustness.

In [21], the authors proposed a new method to embed secret data in the GREEN or BLUE channel of carrier image on the basis of secret key bits and RED channel LSB. This method adds one more level security to the existing LSB method by utilization of secret key. The RED channel LSB and secret key bit is cored and then a decision is taken on the basis of its result to replace the LSB of GREEN or BLUE channel. The proposed method has the same payload, more robustness and better security as compared to simple LSB method. However the secure key exchange of secret key is an open challenge and is an extra overhead of proposed method.

Ibrahim and Kuan have developed a SIS (Steganography Imaging System) in [22] which uses a secret key to enhance the security of the proposed system. The authors have made use of zipping to zip the secret key and secret data in order to increase the payload. The zip file is then converted into bits stream and hidden in cover image. The proposed algorithm has high payload capacity and better quality of stego images but this technique is proposed only for BMP format images.

**Proposed Algorithm:** All the communicating bodies want the confidentiality, integrity and authenticity of their secret information. Different approaches are used to cope with these security issues like digital certificate, digital signature and cryptography. But these methods alone cannot be compromised. Steganography is the best solution to these problems as it hides the existence of secret data. This paper proposes a novel image steganography LSB based technique for RGB images using color space exchanging from RGB to HSI. The secret data is embedded in I-Plane of HSI color model using LSB method. Finally the resultant image is retransformed to RGB color model to make the stego image.

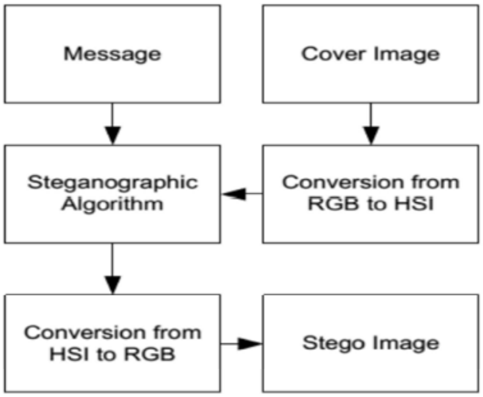

Fig. 2: Proposed Model of Steganography

**Color Models:** Color models are also known as color systems or color spaces. The main goal of these color spaces is to represent all colors in a standard way. A color model is a way of representing a set of colors mathematically. The most popular color spaces are RGB, YCbCr (Luminance Component, Chroma Blue difference, Chroma Red difference) and CMYK (Cyan, Magenta, Yellow and Black), HSI (Hue, Saturation and Intensity).

The HSI color model is derived from RGB color space that represents colors the way the human eyes perceive and interpret colors. Human eye describes colors by its hue, saturation and intensity. Hue represents a pure color i.e. pure red, yellow etc. Saturation gives us a measure of the degree to which a pure colour is diluted by white light. Intensity is the brightness of a color [23, 24].

**Why HSI Color Model for Embedding:** The proposed method uses HSI color space for information hiding because of the following reasons.

- Processing an image in RGB color system is relatively more difficult and time consuming. All the three values of a particular pixel need to be read, the intensity is then calculated, the desired changes is made, new RGB values are recalculated and stored.
- The brightness information in RGB color space is embedded in its each layer which indicates that all the three layers are strongly correlated to one another and any changes to one of its layer will have its corresponding effect on other layers.

**Conversion from RGB to HSI:** The image in RGB color space is transformed into HSI color space by the following formulae.

$$r = \frac{R}{R+G+B} \tag{1}$$

$$g = \frac{G}{R+G+B} \tag{2}$$

$$b = \frac{B}{R+G+B} \tag{3}$$

$$h = \cos^{-1}\left[\frac{0.5\times\{(r-g)+(r-b)\}}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\right] \tag{4}$$

$h \in [0,\pi]$ for $b \leq g$

$$h = 2\pi - \cos^{-1}\left[\frac{0.5\times\{(r-g)+(r-b)\}}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\right] \tag{5}$$

$h \in [\pi, 2\pi]$ for $b > g$

$s = 1 - 3 \times \min(r, g, b)$

$s \in [0,1]$

(6)

$$i = \frac{R+G+B}{3\times 255} \; i \in [0,1] \tag{7}$$

For the sake of convenience h, s and i values are transformed into these ranges [0,360], [0,100], [0, 255], respectively by:

$$H = \frac{h\times 180}{\pi} \tag{8}$$

$$S = s \times 100 \tag{9}$$

$$H = h \times 255 \tag{10}$$

**Conversion from HSI to RGB:**

$$h = \frac{H\times\pi}{180} \tag{11}$$

$$s = \frac{S}{100} \tag{12}$$

$$i = \frac{I}{255} \tag{13}$$

$$x = i \times (1 - s) \tag{14}$$

$$y = i \times \left[1 + \frac{s\times\cos(h)}{\cos(\frac{\pi}{3}-h)}\right] \tag{15}$$

$$z = 3i - (x + y) \tag{16}$$

If $h < \frac{2\pi}{3}$ then b =x, r =y and g =z

If $\frac{2\pi}{3} \leq h < \frac{4\pi}{3}$ then $h = h - \frac{2\pi}{3}$, r =x, g =y and b = z

These are the normalized values of r, g and b in the range [0, 1]. Finally these values are multiplied by 255 in order to form the original RGB values[23].

**Embedding Algorithm:**
**Input:** Cover Colour Image, Secret data
**Output:** Stego Image

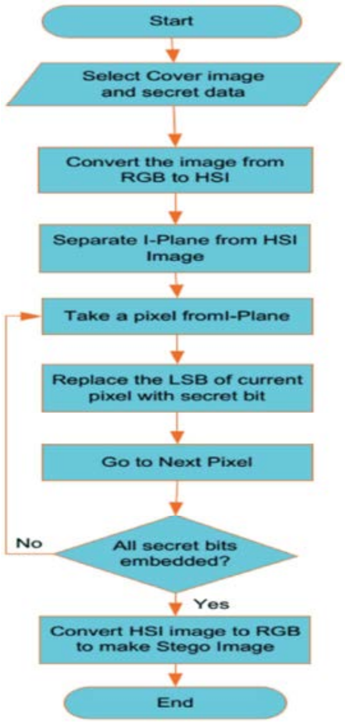
Start
Select Cover image and secret data
Convert the image from RGB to HSI
Separate I-Plane from HSI Image
Take a pixel fromI-Plane
Replace the LSB of current pixel with secret bit
Go to Next Pixel
No
All secret bits embedded?
Yes
Convert HSI image to RGB to make Stego Image
End

Fig. 2: Embedding Algorithm Flowchart

Step 1 : Take the cover RGB image and secret data.
Step 2 : Convert the RGB image into HSI color model using section 3.1.2 formulas.
Step 3 : Convert the secret data into 1-D array of bits.
Step 4 : Take a pixel from I-Plane and replace its LSB with a secret bit.
Step 5 : Repeat Step 4 until and unless all secret bits are encoded in the I-Plane pixels.
Step 6 : Convert the HSI image into RGB color space using the formulae of section 3.1.3.
Step 7 : Write the stego image.

**Extraction Algorithm:**
**Input:** Stego Image
**Output:** Secret data

Step 1 : Take the stego image and convert it into HSI color space.
Step 2 : Consider the I-Plane only for extraction of secret data.
Step 3 : Extract the LSB of current pixel from I-Plane of HSI image.
Step 4 : Repeat Step 3 until and unless all secret bits are decoded.
Step 5 : Convert secret bits into secret data i.e. text, image etc.

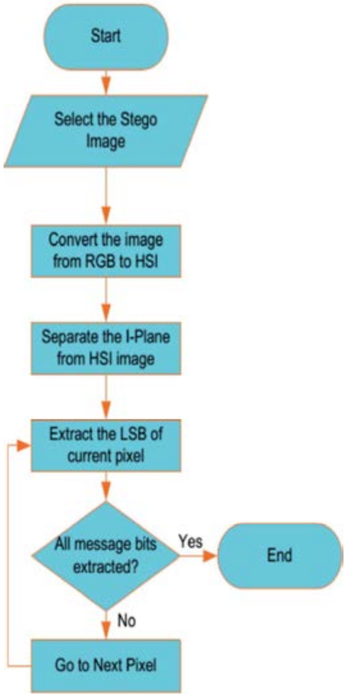
Start
Select the Stego Image
Convert the image from RGB to HSI
Separate the I-Plane from HSI image
Extract the LSB of current pixel
All message bits extracted?
Yes
End
No
Go to Next Pixel

Fig. 3: Extraction Algorithm Flowchart

## RESULTS AND DISCUSSION

The proposed method, LSB technique and technique in [21] are simulated using MATLAB R2013a. For experiments we have embedded variable amount of cipher in different standard color images of same and different dimensions to estimate the performance of the proposed technique. The proposed technique is evaluated by 3 different perspectives; hiding the same amount of cipher in different images of the same dimensions; hiding variable amount of cipher in the same image of the same dimension and hiding same amount of cipher in the same image of different dimensions. The standard color images used for experiments are lena.png, baboon.png, peppers.png, trees.tiff etc.

**Comparison of Proposed Method with Existing Methods:** The comparison among proposed algorithm, simple LSB and algorithm in [21] is based on two types of analysis named as subjective analysis and objective analysis. Subjective analysis is done using Human Visual System (HVS) to notice the changes between the cover and stego images and their corresponding histograms. A few samples of standard color cover and stego images and their histograms for the proposed method are shown below in Figure 9, Figure 10 and Figure 11. From figures it is observed that there is no noticeable change in the cover and stego images and their histograms which shows the effectiveness of the proposed method [22-25].

Objective analysis is a mathematical standard for measuring the distortion that occurs in the cover image after embedding secret data. Objective analysis is performed on the proposed method using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). The PSNR and MSE are calculated by the following formulas of (17) and (18).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{C_{max}{}^{2}}{\mathrm{MSE}}\right) \quad (17)$$

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right) \quad (18)$$

Table 2: Comparison of proposed method with LSB and Method in [21] based on PSNR

| | LSB Method | Karim's Method[21] | Proposed Method |
|---|---|---|---|
| Image Name | PSNR (dB) | PSNR (dB) | PSNR (dB) |
| baboon.png | 61.8784 | 48.558 | 94.4421 |
| lena.png | 42.6331 | 42.6204 | 42.5417 |
| peppers.png | 62.9666 | 17.39 | 100 |
| building.png | 51.4677 | 47.0305 | 70.0942 |
| parrot.png | 49.708 | 49.8421 | 62.4971 |
| trees.tiff | 63.46 | 50.5301 | 83.9069 |

Table 3: Comparison based on PSNR with variable amount of cipher embedded

| | | LSB Method | Karim's Method [21] | Proposed Method |
|---|---|---|---|---|
| Image Name | Cipher size in (KBs) | PSN dB) | PSNR dB) | PSNR (dB) |
| baboon with dimension 256×256 | | | | |
| | 2 | 63.3775 | 52.0373 | 83.6503 |
| | 4 | 61.8442 | 51.6345 | 78.4215 |
| | 6 | 60.4909 | 51.1776 | 74.3139 |
| | 8 | 59.7481 | 50.8811 | 73.6444 |

Table 4: PSNR based comparison with same size cipher and different image dimensions

| Image Dimensions | LSB Method<br>PSNR(dB) | Karim's Method [21]<br>PSNR(dB) | Proposed Method<br>PSNR (dB) |
|---|---|---|---|
| 128×128 | 70.3187 | 65.5328 | 47.1518 |
| 256×256 | 61.8784 | 50.8811 | 73.6444 |
| 512×512 | 52.4555 | 37.2456 | 86.3986 |
| 1024×1024 | 59.204 | 41.9577 | 65.2814 |

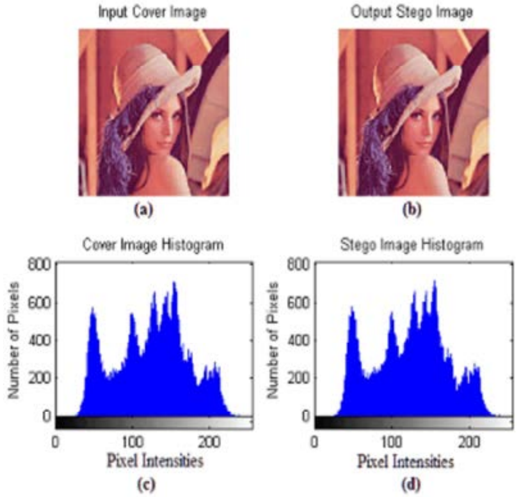

Fig. 9: Lena cover and stego image and their histograms

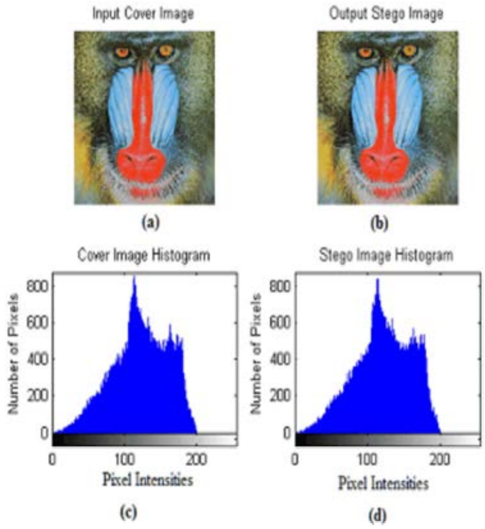

Fig. 10: Baboon cover and stego image and their histograms

Note that here M and N are image dimensions, x and y are loop variables, S is stego image, C is cover image and $C_{max}$ is the maximum pixel intensity among both images [25-30]. The experimental results of the proposed methods, LSB and method in [21] are shown in Table 2, Table 3 and Table 4 respectively.

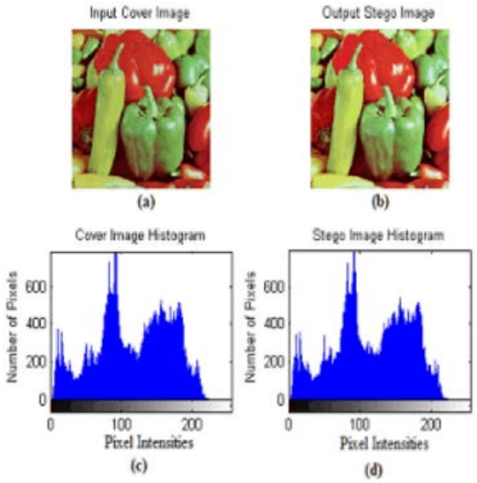

Fig. 11: Peppers cover and stego image and their histograms

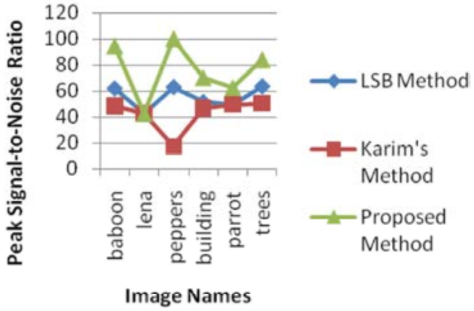

Fig. 12: Comparison based on PSNR with different images of dimension 256×256

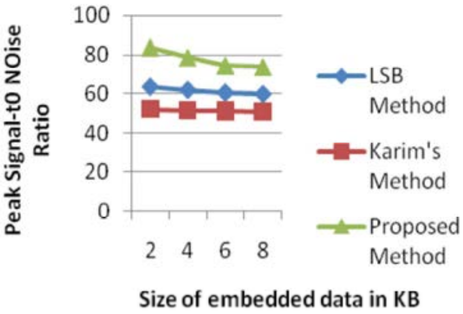

Fig. 13: Comparison based on PSNR with same image dimension and variable amount of cipher

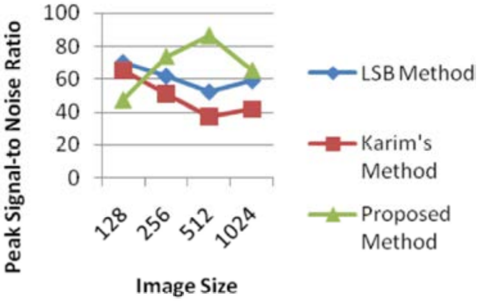

Fig. 14: PSNR based comparison with same size cipher different image dimensions

## CONCLUSION

This paper proposed a novel approach of image steganography for true color images with better imperceptibility, security and robustness. The said approach uses the HSI color model to hide secret messages inside color images to increase the security of the proposed technique. An average PSNR of 75.57dB is achieved with this novel approach which shows the superioty of the proposed method as compared to existing methods. This method introduces and adds an extra security level barrier in the way of an attacker which makes the attack on this algorithm awful and misguides the process of steganalysis.

## REFERENCES

1. Hussain M. and M. Hussain, 2013. A Survey of Image Steganography Techniques, International Journal of Advanced Science and Technology, pp: 54.
2. Ramaiya, M.K., N. Hemrajani and A.K. Saxena, 2013. Security Improvisation in image Steganography using DES, in Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp: 1094-1099.
3. Kumar, V. and D. Kumar, 2010. Performance evaluation of dwt based image steganography," in Advance Computing Conference (IACC), 2010 IEEE 2nd International, pp: 223-228.
4. Babu, K.S., K. Raja, K. Kiran, T. Manjula Devi, K. Venugopal and L. Patnaik, 2008. Authentication of secret information in image steganography, in TENCON 2008-2008 IEEE Region 10 Conference, pp: 1-6.
5. Jabeen, F.Z. Jan, A. Jaffar and A.M. Mirza, 2010. Energy Based Coefficient Selection for Digital Watermarking in Wavelet Domain, in Information Computing and Applications, ed: Springer, pp: 260-267.
6. Abbasi, A.Z. Jan and A. Jaffar, 2010. Genetic Programming based Robust Image Watermarking using wavelet and Morton order.
7. Jan, Z.F. Jabeen, A. Jaffar and A. Rauf, 2010. Watermarking scheme based on wavelet transform, genetic programming and Watson perceptual distortion control model for JPEG2000, in Emerging Technologies (ICET), 2010 6th International Conference on, pp: 128-133.
8. Cummins, J.P. Diskin, S. Lau and R. Parlett, 2004. Steganography and digital watermarking, School of Computer Science, The University of Birmingham, 14: 60.
9. Kavitha, K.K., A. Koshti and P. Dunghav, 2012. Steganography Using Least Significant Bit Algorithm, International Journal of Engineering Research and Applications (IJERA), issn, pp: 2248-9622,
10. Kumar, A. and K. Pooja, 2010. Steganography-A Data Hiding Technique," International Journal of Computer applications, 9: 19-23.
11. Akhtar, N.P. Johri and S. Khan, 2013. Enhancing the Security and Quality of LSB Based Image Steganography," in Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, pp: 385-390.
12. Balakrishna, C.V. Naveen Chandra and R. Pal, 2013. University of Hyderabad, Hyderabad, India," in India Conference (INDICON), 2013 Annual IEEE, pp: 1-4.
13. Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt, 2010. Digital image steganography: Survey and analysis of current methods, Signal processing, 90: 727-752.
14. Samima, S.R. Roy and S. Changder, 2013. Secure key based image realization steganography, in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on, pp: 377-382.
15. Tilakaratne, U. and U. Pinidiyaarachchi, 2013. Image steganography scheme based on reversible data embedding strategy, in Computer Science and Education (ICCSE), 2013 8th International Conference on, pp: 503-507.

16. Thenmozhi, S. and M. Chandrasekaran, 2013. A novel technique for image steganography using nonlinear chaotic map, in Intelligent systems and control (ISCO), 2013 7th international conference on, pp: 307-311.
17. Jan, Z. and A.M. Mirza, 2012. Genetic programming-based perceptual shaping of a digital watermark in the wavelet domain using Morton scanning, Journal of the Chinese Institute of Engineers, 35: 85-99.
18. Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography," Journal of Emerging Technologies in Web Intelligence, 2: 56-64.
19. Amirtharajan, R.P. Archana, V. Rajesh, G. Devipriya and J. Rayappan, 2013. Standard deviation converges for random image steganography, in Information and Communication Technologies (ICT), 2013 IEEE Conference on, pp: 1064-1069.
20. Grover, N. and A. Mohapatra, 2013. Digital Image Authentication Model Based on Edge Adaptive Steganography, in Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on, pp: 238-242.
21. Karim, M., 2011. A new approach for LSB based image steganography using secret key, in 14th International Conference on Computer and Information Technology (ICCIT 2011), pp: 286-291.
22. Ibrahim, R. and T.S. Kuan, 2011. Steganography Algorithm to hide secret message inside an Image,arXiv preprint arXiv: 1112.2809.
23. Gonzalez, R.C., R.E. Woods and S.L. Eddins, 2004. Digital image processing using MATLAB: Pearson Education India.
24. Sebastian, P., Y.V. Voon and R. Comley, 2010. Colour space effect on tracking in video surveillance," International Journal on Electrical Engineering and Informatics, 2: 298-312.
25. Wang, Z.E., P. Simoncelli and A.C. Bovik, 2003. Multiscale structural similarity for image quality assessment,in Signals, Systems and Computers, 2004. Conference Record of the Thirty-Seventh Asilomar Conference on, pp: 1398-1402.
26. Zhang, L., D. Zhang and X. Mou, 2011. FSIM: a feature similarity index for image quality assessment," Image Processing, IEEE Transactions on, 20: 2378-2386.
27. Wang, Z., A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, 2004. Image quality assessment: from error visibility to structural similarity,Image Processing, IEEE Transactions on, 13: 600-612.
28. Silva, E.A., K. Panetta and S.S. Agaian, 2007. Quantifying image similarity using measure of enhancement by entropy, in Defense and Security Symposium, 65790U-65790U-12.
29. Mittal, A., R. Soundararajan and A.C. Bovik, 2013. Making a “completely blind” image quality analyzer, Signal Processing Letters, IEEE, 20: 209-212.
30. Fang, Y.K. Zeng, Z. Wang, W. Lin, Z. Fang and C.W. Lin, 2014. Objective Quality Assessment for Image Retargeting Based on Structural Similarity, IEEE J. Emerg. Sel. Topics Circuits Syst., 4: 95-105.