EA based Heuristic Segmentation for Efficient Data Hiding

Raniyah Abdullah Wazirali

Centre for Real-time Information Networks (CRIN)
Faculty of Engineering and Information Technology (FEIT)
University of Technology, Sydney (UTS)

Zenon Chaczko

Centre for Real-time Information Networks (CRIN)
Faculty of Engineering and Information Technology (FEIT)
University of Technology, Sydney (UTS)

ABSTRACT

Information concealment is of paramount importance in information and communication security. For the protection of information and intellectual property, effective techniques are needed. Steganography is the art of writing concealed information in a way that it does not arouse suspicion about its existence. This ensures that only the sender and the recipient are aware of the concealed message existence. Capacity and Stego image imperceptibility are the most crucial aspects. This paper provides a heuristic approach of choosing the right-most regions for embedding that ensure minimum changes to stego object. Then, different percentages of secret data will be hidden on the cluster based on the characteristic of the region. Therefore, the sharp edge region will hide more data while the smooth will hide data. The proposed approach use K-mean clustering to categorized the segmentation and then genetic algorithm will be used to boost the PSNR (peak signal to-noise ratio) value while optimizing high capacity information. The obtained stego object is virtually indistinguishable from the cover object. The experimental results show a significant enhancement over other previous work.

General Terms:

Data Hiding, Information Security

Keywords:

Steganography, LSB, K-mean clustering, GA

1. INTRODUCTION

Steganography is the science of hiding information within another, steganographic system basically embedding secret file in cover carrier media without arising attacker suspicion [2]. Steganographic system has two main criteria which are payload capacity and stego image quality. However, steganographic payload capacity and vagueness are at conceivable outcomes with one another. For example, hiding more subtle elements in secure pictures (higher capacity) exhibits more relics into the carrier file and thus increasing the distortion of the hidden information and therefore decrease the quality of the stego file . The steganographic techniques can be categorized as follows:

High embedding capacity techniques with acceptable stego object imperceptibility. In this type, the embedding mechanism func-

tions on each pixel without taking into consideration the rightmost place to embed the data. The most common technique for this type is the Least Significant Bits substitution technique (LSB). In LSB, the secret messages are hidden in the least significant bits for each pixel to create the stego file. As the alteration is made in the LSB part, the human eye can not preceive the changes of the stego object. However, with the increase size of the secret file, more LSBs must be altered and therefore effecting the visual quality. Generally, the LSBs based approach allows hiding higher secret file size as compared to other techniques.

Secondly, moderate payload capacity with high stego object imperceptibility. In this category, the main target is to preserve the characteristics of the original image. Basically, the embedding of the secret message based on the variation among the neighbor pixels. Therefore, in this type the secret data embedded in some specific region based on the characteristic of the region. [5, 13, 11] are a few adaptive steganographic techniques that take into consideration human vision sensitivity as well as local texture characteristics. Moreover, edge based steganographic approach can be classified in this category. Thirdly, high embedding efficiency with a minor alteration. This type focuses on minimizing the stego file degradation when embedding small amount of secret message, normally one or two bits per pixel. The embedding efficiency can be considered as the ration between the amount of the embedded bits and the related degradation caused by the embedding technique. Zero-steganography is an approach developed to provide invisibility which produce immune to steganoaysis [3].

This paper focuses on the second category of steganography techniques and practically, intends to enhance adaptive steganography. The work focus on providing heuristic scheme for color images that can both optimize the payload capacity and produce an indistinguishable stego image from the original cover image in an acceptable computation time. To achieve optimal result, the work must evaluate each possible substitution, which could involve a huge amount of processing and computation time and therefore, provide unacceptable approach. To overcome this issue, evolutionary computation technique that utilized GA will be used. The benefits of using GA along with k mean clustering and normalized cuts include the following; (1) high capacity capability and the stego object does not degraded significantly; (2) the selection of region is randomized which make the extraction process difficult and therefore meaningless to the attacker. (3) due to the use of GA, the computation time is acceptable. The experimental results will prove the given advantages. The rest of this paper can be organized as follows. The description of the related works given in section 2. Section 3 explains the proposed method that include the segmentation approach based on clustering part followed by the region selection using GA and then embedding different amount of the secret message based on the characteristic of the region. Section 4 will evaluate the results of the proposed method and compare it with some classical works.

2. RELATED WORKS

In order to obtain high payload capacity with least changes, the secret message should be embedded carefully in some specific region based on the characteristics of the host image. Because of the simplicity of edge detection approach, its provide robust hiding techniques against attacks as preserving the abrupt modification in image intensities. Wu and Tasi (2003) proposed pixel-value differencing (PVD) scheme that use the difference value between two pair pixels as the size of the embedding capacity[13]. The main concept of PVD based on exploiting the differences values to insert the secret message. The amount of the differences indicates the secret message and assist to keep the degree of the differences unmodified after embedding the information. In PVD the difference values are categorized and allocated to some different grades, then higher grade specifies a larger dissimilarity value and the lower grades shows least differences. Fundamentally, a higher difference between two consecutive pixels means that these two pixels are more proper for modification of embedding some data. If two consecutive pixels have a slight different values, then only small amount of data can be embedded in this pair because it is allocated in a smooth region and therefore any changes can degrade the visual quality. In 2010, Singh et al. proposed a novel technique for hiding secret message in digital color image based on LSB replacement[9]. The method based on modifying a few pixel color value that use some selected pixel to represent characters instead of color value and this lead to high visual quality of stego object. Many adaptive steganographic techniques take into consideration human vision sensitivity as well as local texture characteristics [5, 13]. Moreover, edge based steganography approaches can be classified in this type. Chen et al. used hybrid edge detector that combines fuzzy edge detection with canny edge detector [12]. Yogarajah et al. used skin detection method to hide the secret message in skin area [15]. Nitin et al. and Basil et al. used canny edge detector to detect edge regions and embed the data using k LSBs [8, 16]. However, Sneha et al. utilized edge detection scheme based on 3x3 window and secret message embedded in edge region using first component modification method [1]. Bassil et al. provides an algorithm that is categorized by three parameters which are the size of the of Gaussian mask, low threshold value and finally high threshold value [16] . These parameters can lead to various outputs of the same carrier and secret message. Wazirali et. al 2014 [11] used score matrix with GA to evaluate wheather the specific block belong to sharp region or smooth.

3. PROPOSED METHOD

In order to optimize the imperceptibility in spatial domain techniques while keep high payload capacity, Genetic Algorithm (GA) with clustering steganography scheme has been developed. Most of spatial domain techniques assume that the least significant bits of the cover image is random and insignificant. Thus, the set of pixels for data embedding can be chosen randomly using Pseudo Random Number Generator (PRNG). This assumption can not be always true, especially for cover images that have high proportion of smooth areas. In fact, there are some differences of the smooth re-

gions and sharp regions. The sharp edge regions present more complicated features, hence more difficult to detect changes in this regions. This section proposes new heuristic segmentation approach for data hiding. The proposed method mainly divided into three main phases, segmentation phase, region selection phase and hiding phase. Figure 1 show the main process of the reusable software architecture. Depending on the input artifact, various variability of the algorithm can be applied which can provide high capability of the output stego objects.

3.1 Segmentation Phase

As normalized cuts standard interpretation image as graph, every linked combined of pixels are measured, image with size of $m \times n$ will necessitate the normalized cuts process to concept a W matrix with size $(m \times n) \times (m \times n)$ pixels. For instance, image with size 512×512 pixels will require 262144×262144 operations. This number of computing require giant computer memory storage to solve this huge size matrix and require a time. This problem could impede the eigenvalue problem solving. Therefore, it is important to re-size the image into smaller groups of pixels to image segmentation. In the proposed method, image segmentation divided into two stages that are making image cells followed by segment merging.

The cover image has been divided into equal size of sub-images that are called image cell. For each images cell, the work starts with independent local division. In order to divide out k number of segments, normalized cuts algorithm is performed using k - meanclustering. Clustering is the process that follows the normalized cuts. Clustering mainly focuses on dividing the connection of input dataset and recovering data points demonstrating each cluster or group. Clustering comprises dividing a group of patterns into a smaller number of groups that are similar with respect to the appropriate relationship measure; for instance, similar patterns are categorized into the matching clusters. Then, an initial check is flicked through every image cell to control if particular cell is essential to get segmented or not. Therefore, no division will be performed in smooth area where all the values of the image cell are similar and thus the image cell will only reflect a segment. In addition, over-segmentation is likely to occur as taste degree in an image cell as compact as compared to whole image directly. However, the over segmentation will assist to decrease the slope of segmented object margins to create better segmentation. Generally, it is independently performed the segmentation in the cells. Segmented groups from the process of image cells and the segments merging phase is begun. The normalized cut standard calculates both the overall dissimilarity between the various image cells as well as the overall similarity within the image cells.

Homogeneous areas of an image are areas holding common features and are gathered as single cluster. After the processing of building image cell, each segment is characterized by nodes holding the average value of the pixels of color brightness in the segments and centroid position of the segments. The total number of the nodes represents the number of segments created from image cell stage. For instance, 40 segments performed from image cells will have 40 nodes. Then normalized cuts algorithm is performed in the computed nodes. Finally, segments from image cell will merged together if their nodes have similar property based on the color value and centroid position attributes.

3.2 Region Selection Phase

In order to obtain high imperceptibility of the stego object, the message will be embedded in selected regions and therefore, providing

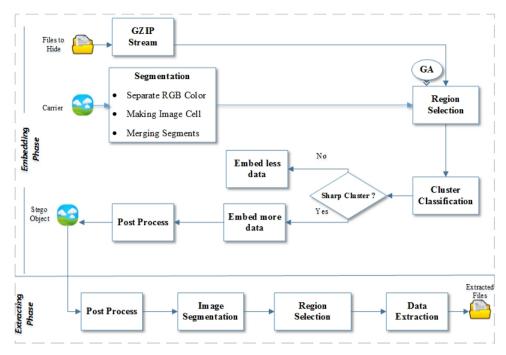


Fig. 1: Reusable Software Architecture for Steganographic Embedding Information Approach

the maintenance of the cover image statistical features. Seeing how the spatial domain embedding approaches, which does not allow for choosing the given position due to the regularity of message distribution, embedding the message in a certain location will be fraught with a number of difficulties, such as the definition of changes in the spatial project. In the project in question, the mapping technique is going to be used in order to split the cover image under consideration into several major block clusters and, thus, perform an analysis, since the aforementioned approach will help place every single element of the message in its place. The above mentioned operation will contribute to define the most reasonable frequency domain position and, thus, drive the number of static feature disturbances on the chosen spatial domain slot to minimum, in order to choose the rightmost region for hiding the message M, the threshold Tcan be obtained in each region based on its characteristic.

To obtain the goal of optimizing the stego image imperceptibility while keeping high payload capacity, the work involves testing PSNR for hiding the secret message in each possible region with the highest possible percentage of k LSB. However, when k is greater than 3, the number of possible substitution is very high. For instance, when k=4 then, there are $(2^4)!=(16)!=20,000$ billions of substitutions which can be tested for hiding the data. Therefore, the computation of PSNR value for each substitution is very time consuming hence unacceptable. A genetic algorithm can be used to overcome this issue.

The genetic algorithm (GA) is a search and optimization approach founded on the doctrines of natural selection and genetics. It enables population involving may people to evolve under itemized selection rubrics to a state which makes the most of the ?fitness? while minimizing the cost function. The technique was advanced by John Holland in 1992 [7]. The algorithm begins with no knowledge if the right solution and relies completely on responses from the surrounding environment, evolution operators: crossover, reproduction and mutation, to attain the right solution [4].

In utilizing genetic algorithm for resolving an assured type of issue, the first stage is to transform some applicant results to the issue into chromosomes including many genes. Based on the operations of reproduction, mutation and crossover, the GA becomes several chromosomes. Those chromosomes are the applicant results of the issue. A function utilized to evaluate the quality of the produced chromosomes is termed the fitness function. Utilizing the fitness function to evaluate those chromosomes solution, if we can catch a strong chromosome, we are definite to get a good solution. Wang et al. used the GA stages to produce a replacement matrix for resolving the issue of image hiding. Firstly, the applicant substitution matrices should be transformed into chromosomes [10].

The process of Genetic Algorithm can be describe in the below steps: . 1. Creating a random population of chromosomes;

2. Assessing the objective (fitness) function; the evaluation of the given function hinges on the PSNR criterion, which is supposed to reach its minimal value for the process to have any meaningful results. PSNR, or Peak Signal to Noise Ratio, being the criterion as the foundation for the fitness function, it is traditionally defined with the help of the following equations:

$$PSNR = 10 \times \log_{10} \frac{Max^2}{MSE} \tag{1}$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (A_{ij} - B_{ij})^{2}$$
 (2)

The PSNR value is considered to be the fitness function. Any value under 30 dB of PSNR values indicate low quality (i.e., distortion caused by embedding is high). A high and acceptable quality stego image should strive PSNR value of 40 dB, or greater [6]. The higher PSNR value means the minimum changes and the higher

Volume 118 - No. 5, May 2015

quality. The score matrix will evaluate the changes of the cover image for each block.

- 3. Repeating the steps a to c until the new population is made:
- a. Choosing a pair of chromosomes (probability increasing together with the function of fitness);
- b. Forming two new strings with a crossover of chromosomes;
- c. Mutating the newly obtained chromosomes and plant the new strings into the population.
 - 4. Swapping the new and the previous population;
- 5. As long as the optimum solution can be provided by correcting the value of error with the amount of generations or the maximum amount of generations is attained before it ceased to grow at the point where it serves as the location of the best chromosome, the experiment can be considered successful.

3.3 Hiding Phase

Based on the complexity of the selected region, different percentages of LSBs will be applied to embed the secret data. Therefore, the sharp edge region will hide higher percentage, while the smoother will hide less.

As the green color has more visual perception of intensely of the human visual system while the blue has the lowest perception contribution to the color image. Therefore, the last bite of each pixel is the most appropriate bite to hide more data.

In smooth region 2-1-4 embedding technique will be used. 2:1:4 of R:G:B LSBs embedding technique will be used to hide the data in RGB color image respectively. That mean, 2 bits in the least significant bit of the red component, 1 bit in the last LSBs of green component and 4 bits in 4 LSBs of blue component. Therefore, 1 byte will be hidden in each pixel of the smooth region.

In sharp edge region 4-2-6 LSBs embedding technique will be used to hide data that means this region will hide more bits than the smoother region. 4 bits in the LSB of the red component, 2 bits in the last 2 component of green and 6 bits in 6 LSBs of Blue component will be utilized for data embedding. Therefore, 12 bits will be hidden out of 24 bits of each pixel of the complex region.

3.3.1 Post Process. In this post process, an Optimal Pixel Adjustment Process (OPAP) will be used to improve the visual quality of the obtained stego image. In 2004, OPAP had been introduced by Chan et al. [4]. The main idea of OPAP is to do optimal modification with the number of the last significant bits that used to embed the secret message and therefore minimize the distortion as much as possible.

4. EXPERIMENTAL RESULTS

The results achieved throughout the research work indicate that the combination of Graphical User and C# increases the ability to attain the probable results. All the tested image in this experiment are 24 bit color RGB images that 512×512 . The experiments include testing over 6 different cover images ("Lenna", "Pepper", "Airplane", "Baboon", "House" and "Tiffany) with various sizes of secret message. The secret message can be text or image.

The first generation of the proposed method is consists of 10 chromosomes that are produced by random number of clusters to obtain the first population. Then, through each generation three main operators will occur and therefore the solution become more closer to the optimal solution which include, crossover, mutation and reproduction. The resulted chromosomes are then evaluated based on PSNR values and only the top 10 highest PSNR will survive form

the population of next new generation. In the last generation, only chromosomes own highest PSNR value are selected. In this section, the result will be evaluated based on the PSNR value, histogram error and computation time.

4.1 Evaluate the Payload Capacity

Payload capacity is one of the most important criteria to measure and ensure the success of any steganographic system. It is the maximum number of bits that can be embedded in a specific cover image without degrading the preserve quality. It can be calculated using 3 where N is the number of bits of the data message and W,H are the width and height of the cover image. W and H will be 512 in all tested cover images.

$$Capacity = \frac{N}{WH} \tag{3}$$

4.2 Evaluate the Imperceptibility

Since hiding data may cause some noises to the resulted stego object, this noise must not degrade the statistical means neither the perceive quality. Imperceptible system means the degradation between the cover image and the stego image is unnoticeable. Peak Signal to Noise Ratio (PSNR) measures the quality of the resulted stego image based on the measurement of the Mean Square Error (MSE) with respect of the cover image. CPSNR will be used in this study since it gives better result as CPSNR calculates the quality for the color images as given in equation 5 where $MSE_{\tau},\ MSE_{g}$ and MSE_{b} measure the mean square error for red, green and blue respectively.

4 and 6 show the related equations to calculate the PSNR and MSE.

$$PSNR = 10 \times \log_{10} \frac{Max^2}{MSE} \tag{4}$$

$$CPSNR = 10 \times \log_{10} \frac{Max^2}{MSE_r + MSE_g + MSE_b}$$
 (5)

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (A_{ij} - B_{ij})^{2}$$
 (6)

Moreover, as human visual sensitivity could have a various response to red, green and blue light. CHPSNR will be used to mea-

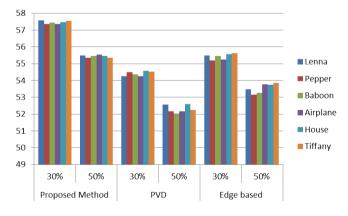


Fig. 4: CPSNR comparison over different embedding capacity of proposed method with others approaches of Lenna amd Pepper image respectively













Fig. 2: The cover images (Lenna, Pepper, Airplane, Baboon, House and Tiffany)













Fig. 3: The resulted Stego images of embedding 50%

sure the imperceptibility since it gives more accurate result based on human visual system where e_{ijkr} , e_{ijkg} and e_{ijkb} measure the error of red, green and blue respectively [14]. CHPSNR =

$$\frac{3 \times m \times n \times Max^2}{\sum_{k} \sum_{i,j} (||h_{ijk} \times (\frac{2}{7}e_{ijkr})||^2 + ||h_{ijk} \times (\frac{1}{7}e_{ijkg})||^2 + ||h_{ijk} \times (\frac{4}{7}e_{ijkr})||^2]} \tag{7}$$

As shown in Table 1 the CPSNR and the CHPSNR are high and acceptable for all tested image for both 30% and 50%. The proposed method provide a noticeable improvement in compare to other methods such as PVD and Edge detection based on Canny.

4.3 Evaluate the Detectibility

Histogram Error (HE) measures the absolute error value between the cover image and the stego image. Histogram Error can be calculated as given in 8 where h_c and h_s indicate the resulted histogram of the cover image and the histogram of the stego image respectively.

$$HE = \frac{\sum_{j=1}^{512} (h_c - h_s)}{512}$$
 (8)

Figure 5 shows the histogram comparison between the original host image and the resulted stego image of embedding 50% of secret message in Lenna, Peppers, Airplane, Babbon, House and Tiffany respectively. The differences between the histogram graphs is very tiny and cannot be observe by the human visual system. Therefore, the proposed technique can be considered as a secure method against the statistical and visual attack.

4.4 Evaluate the GA Performance

To increase the imperceptibility in non-GA techniques, each possible solution to find the best mapping region must be tested and therefore the overall computation time will be huge and unacceptable. In the GA, the parameters are denoted by encrypted binary elements, named ?chromosome? or ?genes? which will be adjusted to maximize the imperceptibility by ensuring best mapping function between the cover image and the secret message with acceptable number of iteration. In this work, good balance kept between the cost of GA for best mapping function selection and the overall completion time.

In the GA preparation procedure, the process selects ten entities for each iteration, through the crossover proportion of 0.25 and mutation proportion of 0.05. The preparation iterations are set to 100. The top five individuals with larger CPSNR and CHPSNR are kept for the new individuals in the next generation.

Table 2 shows the increase of the imperceptibility in term of CP-SNR and CHPSNR with the increase number of iteration.

Table 2.: The CPSNR and CHPSNR under different GA iteration

Iteration	CPSNR	CHPSNR
0	49.358	61.254
25	51.584	63.578
50	53.985	66.584
75	55.754	68.587
100	57.581	71.597

4.5 Evaluate the Computation Time

For any optimal steganographic system, it is significant to observe the total computation time to acquire the embedding and the extracting. Since the evolutionary algorithm based on testing every possible solution to achieve better result which may require a huge computation time, making balance between acceptable imperceptibility and acceptable computation time should be considered. Table 3 shows the processing time of the original LSB substitution and the proposed method. The proposed GA clustering consume almost twice the time of that by the original LSB method. However, the results are still in acceptable method. The computation time can be further improved by using faster computer such as Pentium III PC.

5. CONCLUSION

Security, payload capacity and imperceptibility are the main aspects of any steganographic system. Therefore, inserting the secret message in the sharp region will allow hiding high payload capacity while returning good visual quality. In order to improve the performance of steganographic methods, a clustering with GA based algorithm has been developed which will provide a balanced alternative between payload capacity of standard LSB and security of edge detection based embedding. Genetic Algorithm has been used

Table 1.: The performance of CPSNR, CHPSNR and Histogram Error for various embedded rates for the proposed method and other embedding techniques in Lenna.bmp

		Proposed		PVD		Canny Detection	
image	Embedding Rate	30%	50%	30%	50%	30%	50%
Lenna	CPSNR	57.581	55.487	54.257	52.578	55.487	53.487
	CHPSNR	71.598	68.054	68.484	67.547	69.354	67.487
	Histogram Error	2.15	3.14	3.02	5.25	2.95	4.24
-							
Pepper	CPSNR	57.357	55.365	54.487	52.158	55.184	53.158
	CHPSNR	74.368	69.478	69.458	68.365	70.365	69.489
	Histogram Error	2.25	3.27	3.15	5.35	2.85	4.11
Baboon	CPSNR	57.454	55.458	54.354	52.025	55.457	53.258
	CHPSNR	73.587	70.358	69.987	67.587	71.678	69.236
	Histogram Error	2.22	3.34	3.11	5.42	2.75	4.05
Airplane	CPSNR	57.358	55.546	54.253	52.155	55.258	53.759
	CHPSNR	72.898	69.987	70.158	69.487	70.897	69.515
	Histogram Error	2.22	3.32	3.11	5.42	2.75	4.25
House	CPSNR	57.455	55.458	54.577	52.585	55.577	53.756
	CHPSNR	74.268	70.236	69.489	68.487	71.056	69.364
	Histogram Error	2.19	3.44	3.42	5.57	2.57	4.14
Tiffany	CPSNR	57.545	55.354	54.524	52.244	55.632	53.854
	CHPSNR	73.661	70.249	69.487	68.324	70.548	69.319
	Histogram Error	2.24	3.45	3.54	5.37	2.45	4.15

Table 3.: The computation time for original LSB substitution method

Cover Image	LSB computation time	Proposed method computation time
Lenna	0.28	0.49
Pepper	0.26	0.48
Baboon	0.28	0.50
Airplane	0.33	0.50
Tiffany	0.31	0.51
Building	0.29	0.49

to improve the robustness of the method. Fitness functions evaluate every possible solution based on providing a high peak signal to noise ratio (PSNR) which means less degradation of the result stego object. The proposed method provide a balance between high payload capacity, detectability and computation time.

References

- [1] Sneha Arora and Sanyam Anand. "A Proposed Method for Image Steganography Using Edge Detection". In: *International Journal of Emerging Technology and Advanced Engineering* (2013).
- [2] K. Bailey and K. Curran. "An Evaluation of Image Based Steganography Methods Using Visual Inspection and Automated Detection Techniques". In: *Multimedia Tools and Applications* 31 (2006), pp. 55–88.
- [3] Muhammad Bilal et al. "Chaos based Zero-steganography algorithm". In: *Multimedia Tools and Applications* 72.2 (2013), pp. 1073–1092.

- [4] C. K. Chan and L. M. Cheng. "Hiding data in image by Substitution". In: *simple LSB Recognition*, *Pattern* 37.3 (2004), pp. 469–474.
- [5] C.-C. Chang and H.-W. Tseng. "A steganographic method for digital images using side match". In: *Pattern Recogni*tion Letter 25 (2004), pp. 1431–1437.
- [6] J. Fridrich, M.; Goljan, and Rui Du. "Detecting LSB steganography in color, and gray-scale images". In: MultiMedia, IEEE 8.4 (2001).
- [7] John Holland. Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology. Control and Artificial Intelligence. second edition. Cambridge, MA: MIT Press, 1992.
- [8] Nitin Jain, Sachin Meshram, and Shikha Dubey. "Image Steganography Using LSB and Edge Detection Technique". In: *International Journal of Soft Comput ing and Engineering (IJSCE)* 2.3 (2012).
- [9] Saurabh Singh and Gaurav Agarwal. "Use of image to secure text mes sage with the help of LSB replacement". In: International journal of applied engineering research 1 (2010)
- [10] R.Z. Wang, C.F. Lin, and J.C. Lin. "Image hiding by optimal LSB substitution and genetic algorithm". In: *Pattern Recognition* 34 3 (2001), pp. 671–683.
- [11] Raniyah Abdullah Wazirali, Zenon Chaczko, and Anup Kale. "Digital multimedia archiving based on optimization steganography system". English. In: 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE). IEEE, Feb. 2014, pp. 82–86.

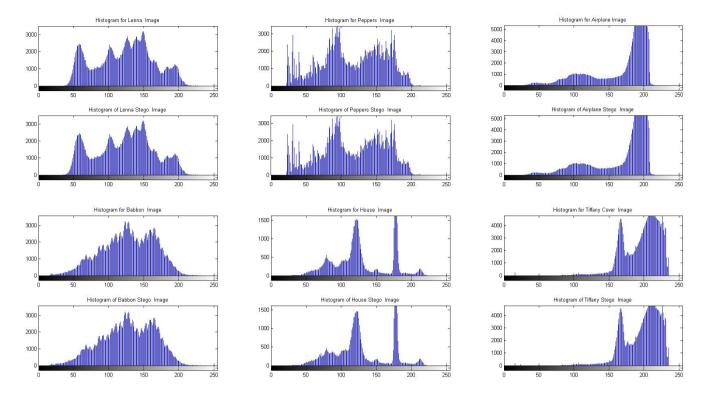


Fig. 5: Histogram Comparison with 50% embedding rate for Lenna, Peppers, Airplane, Baboon, House and Tiffany

- [12] Wen Jan Chen Chang, Chin Chen, and Hoang Ngan. "High payload steganography mechanism using hybrid edge detector". In: *Expert Systems with Applications 37* (2010).
- [13] D.-C. Wu and W.-H. Tsai. "A steganographic method for images by pixel-value differencing". In: *Pattern Recogni*tion Letters 24 (2003), pp. 1613–1626.
- [14] Ma Xiu-ying and Jia-jun Lin. "HVS-Based Imperceptibility Evaluation for Steganography". In: *Institute for Computer Science, Social-Informatics and Telecommunications Engineering* 2 (2009), pp. 152–161.
- [15] Pratheepan Yogarajah et al. "A dynamic threshold approach for skin segmentation in color images". In: 2010 IEEE International Conference on Image Processing. IEEE, Sept. 2010, pp. 2225-2228. URL: http://www.scopus.com/inward/record.url?eid=2-s2.0-78651103034 \&partnerID=tZ0tx3y1.
- [16] Youssef Bassil. "Image Steganography based on a Parameterized Canny Edge Detection Algorithm," in: *International Journal of Computer Applications* 60.4 (2012).