Using Palette and Minimum Spanning Tree for True-Color Image Steganography

SHOW-WEI CHIEN[1,†] , YUNG-FU CHEN[2,†] , PEI-WEI YEN[3], HSUAN-HUNG LIN[4,*]
[1]Department of Information Management, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan, R.O.C
g9523809@yuntech.edu.tw
[2]Department of Health Services Administration, China Medical University, Taichung 40402, Taiwan, R.O.C
yungfu@mail.cmu.edu.tw
[3]Department of Electronic Engineering, Army Academy, Taoyuan 320, Taiwan, R.O.C
pwyen2007@gmail.com
[4]Department of Management Information Systems, Central Taiwan University of Science and Technology, Taichung 40601, Taiwan, R.O.C
shlin@ctust.edu.tw

Abstract: - Steganography is an application of data hiding which can attain camouflage and increase security by embedding the secret message into digital media for sending to the receiver without leaking to the third party. Several proposed methods which construct stegoimage by embedding the secret message into the colour palette. The person who receives the stegoimage can extract the secret message from the palette obtained by the received image. This method, however, greatly degrades the quality of the stegoimage and tends to arouse the intention of the intruders. In this paper, we propose a method for constructing stegoimages with high quality which greatly eliminate the above problem. The advantage of the proposed method is that the image quality is highly improved by accompanying with improvement of security and camouflage of the secret message. In order to avoid the intruder to attack the generated palette when transmission, the sender does not need to send the palette to the receiver directly, but instead asking the receiver to own a copy of the original secret image or obtain one when needed for extracting the secret message. Fortunately, there are several image pools which contain a lot of images allowing to be accessed by the public. The experimental results show that our method outperforms EZ stego and the methods proposed by Fridrich and Wu et al.

Key-Words: - Steganography, Palette optimization, Minimum Spanning Tree

1 Introduction

Digital watermarking and steganography are two applications of information hiding. The former is usually applied to digital library and digital literature for hiding the trademark or logo of an organization inside the media. The latter, on the other hand, is widely used to hide the secret message inside digital media without deteriorating the quality of the media when transmitted on the internet so that it wouldn't evoke the intruder's notice. It not only protects the secret data, but also attains the purpose of concealment. The main considerations about a steganographic algorithm are that the capacity of the hidden secret data should be high enough for embedding the necessary information and the quality of the stegoimage in which the secret information hidden must be good enough to prevent arousing the intruder's attention.

There are many steganographic methods which have been proposed so far. Some of them intended to improve quality of the secret information which have hidden [1-6], some were used to improve the capacity of the secret data been hidden [7], and the others for increasing the protective capability and security [8-9].

Within these steganographic methods, several investigations utilized palettes of the digital images for hiding secret information. A palette is a small set

† The first two authors contributed equally to this work.

* To whom correspondence should be addressed. 11 Buzih Lane, Beitun District, Taichung, 40601, Taiwan, R.O.C.; Tel: 886-4-22391647 Ext.7716; Fax: 886-4-22397919.

of colors used to represent a true-color image so that the amount of data can be reduced. However, using fewer colors to represent a true-color image will degrade the image quality. Therefore palette optimization is generally used to obtain a palette for representing the original image with least error.

Several different kinds of methods, such as c-mean, fuzzy c-mean (FCM) [10-12], and K-mean [13], have been widely applied for training palette by quantization and classification of similar colors into clusters. A palette is obtained by collecting all the centroids of clusters that each is used to represent the cluster. For steganographic applications, after the palette has been obtained, it can be used for hiding secret messages. K-mean algorithm first classifies pixel colors of an image into several clusters that the representative of each cluster is obtained by calculating its centroid. Then, the color palette of an image can be obtained by iteratively assigning each pixel to a cluster which has smallest distance to it. The FCM [10-12] algorithm classifies the *n'* fine colors into *n* coarse colors and calculates the membership matrix at the same time. The optimal solution is obtained by minimizing an objective function which is the weighted sum of squared errors within each group.

1.1 Motivation and goal

EZ stego [3] and the method proposed by Fridrich [2] both utilizes palette to implement steganography. The drawback of these two methods is that image quality of the stegoimage is deteriorated by the number of palette colors, which in turn greatly reduces the capability of camouflage and degrades security. As a result, it might arouse the intension of the intruder to attack and destroy the stegoimage. Although Wu et al. [4] recently proposed an iterative method to obtain a near-optimal palette for improving image quality of the stego image, the problem of limited palette colors in degrading image quality still exists. The quality of a stego image is limited by the number of colors and the quality of the palette of the secret index image. For example, the palettes obtained will be different if different training algorithms are used. As shown in Fig. 1, the difference in image quality can be easily experienced by visual inspection of two images. This visual defect has great influence of security and camouflage in steganography.

In this thesis, although palettes are applied to implement steganography, the original cover image and stego image still keep their true-color form. The advantage of our proposed method is that the image quality is highly attained and accompanied with an improvement of security and camouflage of the secret message. In order to avoid attacking to palette under transmission, the sender does not need to send the palette to the receiver, however the receiver must have a copy of the original secret image to extract the secret message. Fortunately, there are several image pools which contain a lot of images that can be accessed by the public. One can only send the stegoimage to the receiver while obtaining the secret image from the internet or using the one stored in his computer. The experimental results demonstrate that our method outperformes EZ stego and the methods proposed by Fridrich [2] and Wu et al [4] with regard to image quality.

(a)

(b)

Figure 1. (a) True color image. (b) Corresponding index image with 256 colors

1.2 Reversible data hiding and lossless reconstruction

In some cases, not only the secret message contains important information, but also the original cover image. For example, medical images, digital libraries, and document images all contain crucial information for the receiver in addition to the secret message. So the aims of some steganographic methods are the applications about it.

The types of digital image which are used to implement steganography not only include color image and gray image, binary image can also be used to implement steganography. It is more difficult for data hiding and lossless reconstruction of the original images for binary images. Tsai et al. proposed a steganographic method which used binary image [1] for data hiding, based on pair-wise logical computation (PWLC). The mechanism was implemented by incorporating simple logical

operations. It could achieve the benefits of reversible hidden data extraction and lossless reconstruction of original image without utilizing any information from the original image. This method could be applied in document images and binary images. The flowchart of the embedding method is shown in Fig. 2 and the procedure is as follows:

1. Create M-sequence hidden binary bit stream which were transferred by hidden data.
2. Insert a reference bit in front of each bit in the hidden binary bit stream, and group two bits to form a pair.
3. Select suitable places in the original image pair wisely.
4. Perform exclusive-or logical operation for hiding the data.

The mechanism selected the two adjacent pixels with the same value from the original host image as the suitable bit pair, and the logical computation adopt exclusive OR logical operation. The inserted reference bit value is always a "1" and combined with a bit value extracted from the secret message to form a hidden bit pair. The hidden bit pair would do a XOR logical operation with the host image bit pair for hiding the secret message. The detail of message hiding is shown in Table 1.

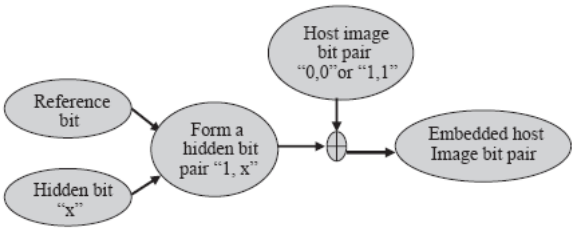


Figure 2. Illustration of PWLC in generating data bit pair to be embedded [1].

Table 1. Data hiding look-up table applied by [1].

Host image bit pair		Embedded data.1		Embedded data.2	
1st pixel	2nd pixel	Reference bit "1"	Hidden bit "0"	Reference bit "1"	Hidden bit "1"
0	0	1	0	1	1
1	1	0	1	0	0

1.3 Application with high capacity and image quality

Risbance et al. [7] addressed that a requirement for steganography is high image quality followed by high embedding capacity. Therefore, the aim of their method was to try to increase the quality of the stegoimage and still maintain a high capacity of hidden message. The method improved the steganography scheme of SMK algorithm [14] by maintaining high embedding capacity while decreasing the distortion [7].

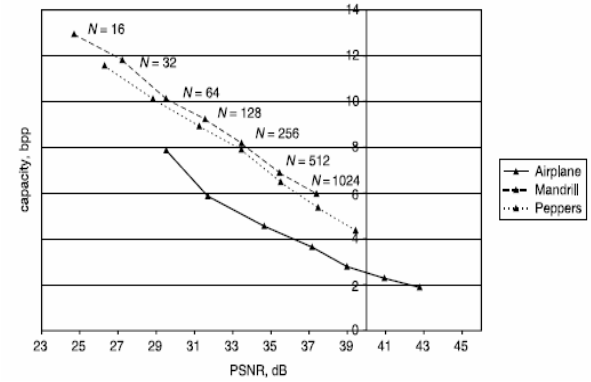


Figure 3. Capacity and imperceptibility of SMK algorithm [11].

Fig. 3 shows the results of implementation of the SMK algorithm, in which N indicates the number of colors of the palette. As shown in this figure, the image quality is degraded if it had higher capacity. The method proposed by Brisbance et al. [7] decreased the distortion and still maintained a high embedding capacity. The embedding algorithm was modified only to embed in the pixels which provide the best tradeoff of capacity and imperceptibility. The benefit of a pixel was defined as the ratio of embedding capacity to the estimated distortion caused by embedding. The average distortion when a pixel p was used for embedding was calculated by Eq. (1)

$$\Delta p = \frac{1}{v_{C(p)}} \sum_{\forall p \in S_{C(p)}} D(p,q) \tag{1}$$

where $C(p)$ is the index of the color palette that the pixel p being contained and $V_{C(p)}$ indicates the number of pixels in the coding structure $S_{C(p)}$ that $S_{C(p)}$ is a set of pixels contained in $C(p)$ and it would be used to hide the secret message in SMK algorithm [11]. The benefit of p was calculated by Eq. (2)

$$B(p) = \frac{h_{c(p)}}{\Delta p} \tag{2}$$

where $h_{C(p)}$ is the embedding capacity for pixel p. Pixels which have a higher benefit are more suitable for embedding. In embedding step, all pixel p,

which has enough benefit, in every indices of color palette would have a label to express the secret bit values, and the pixel *p* would be replaced with other pixel *p'* whose label corresponding with the secret bit values. Although this higher imperceptibility was obtained at the cost of capacity, the capacity could be increased relative to a fixed level of imperceptibility.

1.4 Palette-based steganography

EZ stego [3] and Fridrich's method [2] are two methods that utilize palette to implement steganography. EZ stego [3] first sorts all the entries of a palette by luminance which is the weighted average of three colors, *R*, *G*, and *B*. Most of the neighboring entries of the palette will be close to each other in the color space after sorting. Each pixel in the image can have a new index, namely luminance index, in the sorted palette after quantification, and then the secret message is embedded into the least significant bits (LSBs) of the luminance indices in a binary form. The original index of a pixel, and hence its color, will be changed since the luminance index will be modified after the secret message has been embedded. Fig. 4 shows the procedure of EZ stego algorithm.

Fridrich's method [2], on the other hand, determines if the condition of $(R+G+B+d) \bmod 2=0$ is met before hiding the message information into a pixel, in which *d* is the bit value of the secret message. If the condition is met, nothing has been changed, if not, a color in the palette that is most similar to the pixel color with the above condition is also satisfied is used to replace it. Fig. 5 shows the embedding procedure of Fridrich's method.

Recently, Wu et al. [4] proposed an iterative method of palette-based image steganography. The drawback of their method is that a true-color image should be converted into index image before secret message hiding. Although the image quality of the stego images is satisfactory according to their reports by comparing the stegoimages and the secrete images, the step of converting true-color into index image significantly degrades the image quality. The quality of a stego image is limited by the number of colors and the quality of the palette of the secret index image. For example, the palettes obtained will be different if different training algorithms are used and the difference in image quality can be easily experienced by visual inspection of two images. This visual defect has great influence of security and camouflage in steganography.

The paper is organized as follow. Section 2, details of the proposed method and its procedure will be mentioned. The experimental results and comparisons with previous investigation will be made in Section 3. Finally, a brief discussion and conclusion will be described in Section 4.

Index	R	G	B
1	3	136	80
2	200	187	97
3	0	0	0
4	255	255	255
.	.	.	.
.	.	.	.
.	.	.	.
255	0	165	1
256	233	100	0

Sort the accoding to luminance.

Index	R	G	B	luminance	New index
3	0	0	0	0	1
1	3	136	80	77.97	2
255	0	165	1	82.61	3
256	233	100	0	140.87	4
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
2	200	187	97	182.17	255
4	255	255	255	255	256

(a)

pixel	Index	New index
1	1	2
2	2	255
3	255	3
4	4	256
.	.	.
.	.	.
.	.	.
k	1	2

Embed secret message and do LSB of the new index.

pixel	index	New index	Secret message	
1	255	3	1	
2	2	255	1	
3	1	2	0	
4	4	256	0	
.	.	.	.	
.	.	.	.	
.	.	.	.	
k	255	3	1	

(b)

Figure 4. Illustration of EZ-stego algorithm [3]. (a) Sorting the palette according to luminance. (b) The original indexes of pixels are changed after the secret information has been embedded.

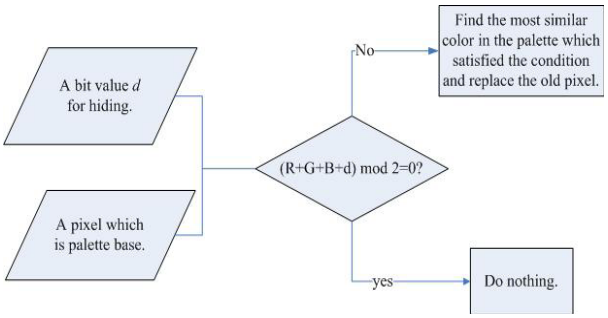


Figure5. Secret message embedding procedure of Fridrich's method [2]

2 Materials and Methods

The palette of an index image is a set of colors obtained by iteratively training a true-color image that the indexes of the palette in turn are used for representing pixel values of the original image. Traditional steganographic methods generally hide

secret information into an index image [2-4]. If someone wants to embed the secret information into a true-color image, the image must be converted to an index image [2-4], which, however, greatly deteriorates the quality of the stego image and can be easily noticed by an intruder. In order to improve the above problem, the method proposed here, like the conventional methods, constructs a palette beforehand. However, instead of embedding the secret message inside an index image, it hides the secret information into a true-color image. The procedure of our proposed method is as follows:

1. Palette training.
2. Construction of a minimum spanning tree for the palette.
3. Determination of the embedding bit value for each nodes based on its level on the tree.
4. Embedding the secret message into the cover image for generating the stego image

For decoding, the receiver must have both the stegoimage and the original image to extract the secret message. Compared to the traditional methods, it seems redundant for our method to transmit stego image accompanied with the original cover image. However, the cover image can be chosen from image pools or databases that are popular or widely known by the community of computer scientist. For this case, the original cover image can be referenced from the receiver's computer or from the Internet so that only the stegoimage is needed to be transmitted to the receiver.

2.1 Palette training

Several popular methods, such as traditional c-mean [13], fuzzy c-mean (FCM) [10-12]) and K-mean [13], have been proposed so far for training the palette. It can be viewed as a special case of the generalized hard clustering algorithmic scheme when data representatives are used and the squared Euclidean distance is adopted to measure the dissimilarity between vectors and cluster representatives. Since K-means algorithm has been utilized extensively by many investigations and its performance is good enough for this study, we therefore utilize K-means algorithm for palette training. The training procedure is illustrated in Fig. 6. The pixel in the original image is consisted of three colors which can be expressed as a three dimensional vector, as expressed in Eq. (3):

$$P = \{p_r, p_g, p_b\} \tag{3}$$

in which pr, pg, and pb indicate the color values of red, green, and blue components, respectively, with each is represented as an 8-bit value. As shown in Eq. (4), K-mean algorithm classifies pixel colors of an image into N clusters that each one is represented as its center of gravity (centroid):

$$\begin{aligned} C &= \{c_1, c_2, c_3, \cdots, c_N\} \\ v_n &= \{v_{nr}, v_{ng}, v_{nb}\} \end{aligned} \tag{4}$$

where the centroid of a cluster, cn, in C is represented as vn. The Euclidean distance between a pixel and the centroid of a cluster can be calculated by the following equation:

$$d = \sqrt{(v_{nr} - p_r)^2 + (v_{ng} - p_g)^2 + (v_{nb} - p_b)^2} \tag{5}$$

After classifying all the pixels based on the initial values generated by a psudo random generator, the new centriod of each cluster can be calculated by averaging the pixel values of each cluster. The procedure is repeated for several iterations until the centroids are stabilized.

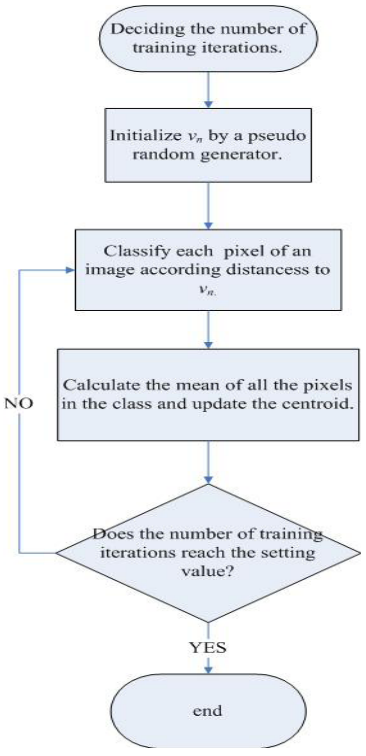


Figure 6. The Procedure of palette training.

2.2 Construction of minimum spanning tree

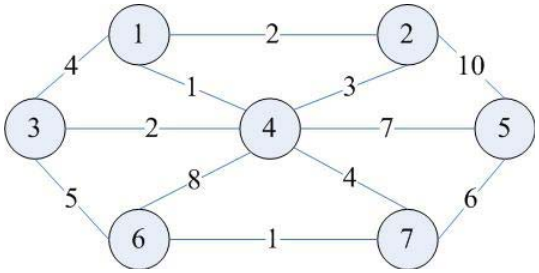
In the design of electronic circuitry, it is often necessary to make the pins of several components electrically equivalent by wiring them together. To

interconnect a set of n pins, we can use an arrangement of $n-1$ wires, each connects two pins. Of all such arrangements, the one that uses the least amount of wire is usually the most desirable.

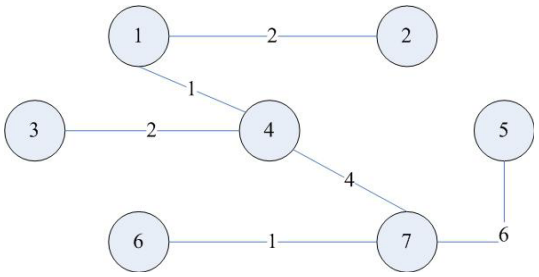
We can model the problem with a connected, undirected graph G= (V,E), where V is the set of nodes, E is the set of possible interconnections between pairs of nodes, and for each edge $(\mu,\upsilon)\in$E, we have a weight $\omega(\mu,\upsilon)$ specifying the cost (distance) to connect μ and υ. We then wish to find an acyclic subset T $\subseteq$ E that connects all of the nodes total weight

$$\omega(T) = \sum_{(\mu,\nu)} \omega(\mu,\nu) \tag{6}$$

is minimized. Since T is acyclic and connects all of the nodes, it must form a tree. It is called a spanning tree [15] since it "spans" the graph G. The problem of determining the tree T is named the minimum spanning tree [15]. An example of connected graph and its minimum spanning tree is shown in Fig. 7.



(a)



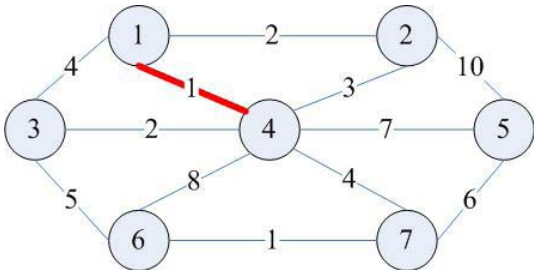
(b)

Figure 7. The graphs (a) before and (b) after executing the algorithm of minimum spanning tree.

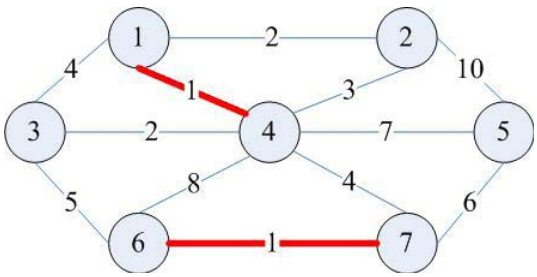
In our proposed method, after the color palette has been trained, it is then used for constructing a minimum spanning tree. In this step, each node will be connected to a spanning tree having the minimum cost to it. In this paper, the node stands for the coefficient, v_n, of the palette, and the cost between two nodes is the Euclidean distance between two coefficients. The method we utilized for constructing the minimum spanning tree is based on Kruskal's algorithm [15].

Kruskal's algorithm [15] is based directly on the generic minimum spanning tree algorithm. It finds a safe edge (μ,υ) with least weight to add to the growing forest by finding all of the edges that connect any two trees in the forest. Let C_1 and C_2 denote the two trees that are connected by (μ,υ). Since (μ,υ) must be a light edge connecting C_1 to some other tree that (μ,υ) is a safe edge for C_1. Kruskal's algorithm [15] is a greedy algorithm, because at each step it adds to the forest an edge of least possible weight. An example is shown in Fig. 8. The algorithm will be repeated until there are N-1 branches that N represents the number of nodes. The detailed algorithm is shown as follow.

```
Procedure Kruskal(G)
  T←0
  while T contains less than n-1 edges do
    choose an edge (μ,υ) from E of lowest cost
    delete (μ,υ) from E
    if (μ,υ) does not create a cycle in T
          than add (μ,υ) to T
    else
          discard (μ,υ)
    end if
  end while
end Kruskal
```



(a)



(b)

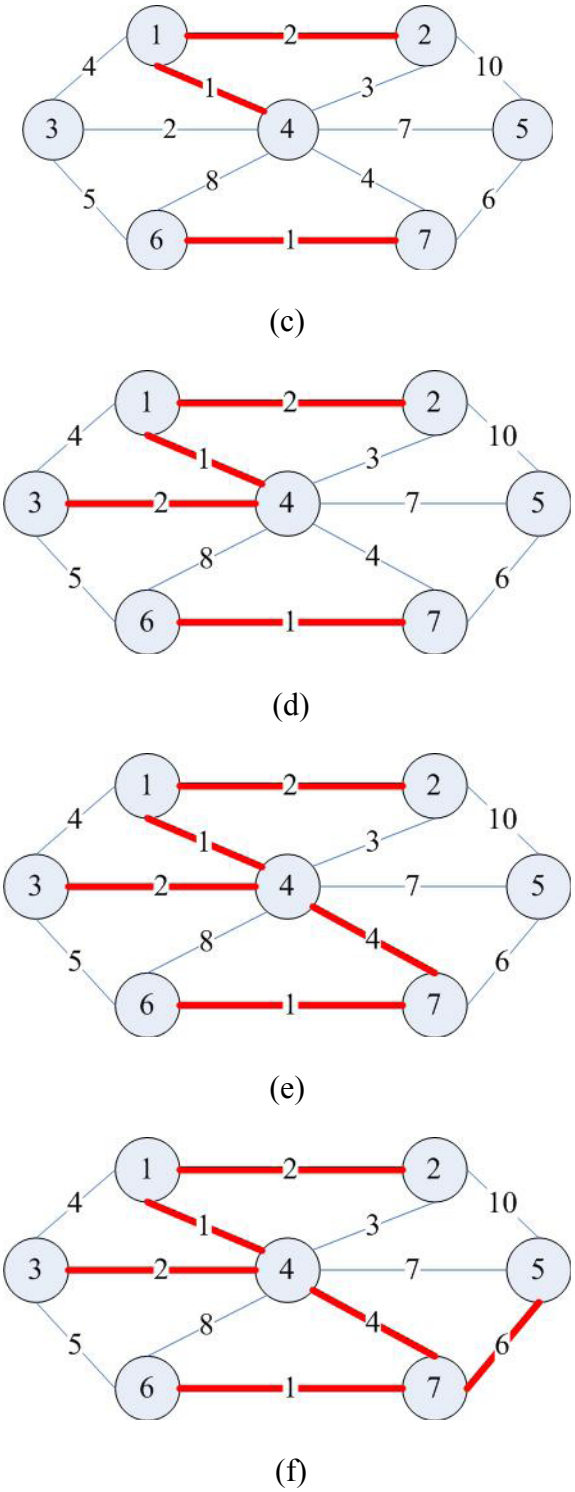


Figure 8. The procedure of Kruskal's algorithm.

2.3 Determination of bit values for nodes of each level

After the minimum spanning tree has been constructed, the embedding bit value (0 or 1) of a node, an entry in the palette, will be embedding. Similar to the traditional method, a bit in the bit string of the secret message will be hidden in a pixel of the secret image. A bit in the secret message will be embedded based on the index (node in the MST) of its corresponding pixel in the secret image. In other word, the level that a node is located in MST determines if the node can embed a 0 or a 1. For example, the root can only embed bit value 0, while the nodes at next lower level can hide value 1, and so on. Hence, as illustrated in Fig. 9, the embedded value of a node is complementary to the values of the nodes one level above and beneath it.

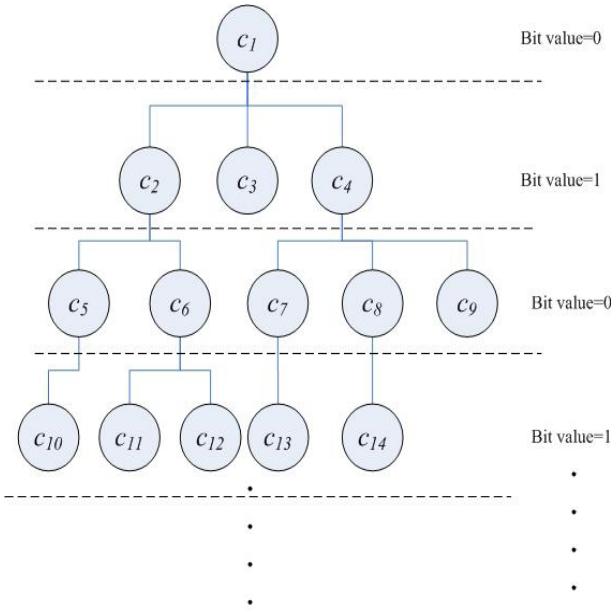


Figure 9. Interleaved assignments of embedding bit values based on which level a node is located in the minimum spanning tree.

2.4 Embedding secret message into cover image

After the palette has been obtained, the minimum spanning tree been constructed, and the bit value of each node been determined, we can start embedding the secret message into a true color image. The secret message is embedded into the cover image bit-by-bit in a raster scanning order, that is, from left to right and top to bottom. In order to build the stegoimage by embedding the secret message bit-wise into a cover image, whether a pixel value is modified (embedding 1) or not (embedding 0) is determined by both the value of a secret bit and the color of its corresponding pixel in which the secret bit is embedded. The procedure is shown in Fig. 10.

As illustrated in the figure, when embedding a bit in the secret message the system first checks if the assigned bit value of the node that the pixel p is classified is same as the secret bit or not. If they are the same, nothing is done; otherwise, modify p to

embed the secret message. The procedure of modifying a pixel p is as follows:

1. Find the node c_A, that the pixel p belongs and find a node (class) c_B which has the minimum cost between them from the minimum spanning tree.
2. Exhaustively search all the pixels which have been clustered in c_B and find a pixel p' which is closest to p, and then replace p with p'.

Since the node c_B is one level above or below c_A in the minimum spanning tree, c_B has complementary assigned bit value to c_A and the cost for replacing p' with p will be minimized. It is different from the method proposed by Wu et al. [4] that the centroid v_B of the cluster c_B is used to replace p. Therefore, our method can achieve better visual quality for the stegoimage.

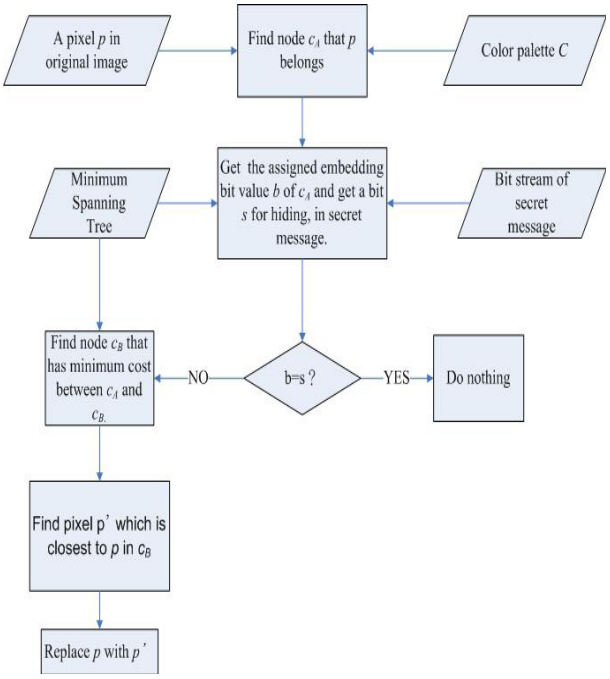


Figure 10. Flowchart of embedding the secret message into a cover image.

2.5 Extracting the secret message from the stegoimage

In order to avoid destroying the palette information by the intruder during transmission, we do not explicitly send the palette to the receiver. Instead, we either send both the stegoimage and the cover image or only the stegoimage. The receiver must have the original cover image, either received from the sender or obtained from the image pools in the Internet or locally in his own computer, to extract the secret message from the stegoimage. From the original cover image, the receiver has to train the palette and build the minimum spanning tree by the same rule applied at the sending side. After assigning the embedding bit value for each node, the receiver is able to extract the secret message from the stegoimage.

3 Experiment Results

In this study, PSNR (Peak Signal to Noise Ratio) between the original image and the stego image is used to evaluate the image quality. It can be calculated from the following equation:

$$PSNR = 10\log_{10}\left[\frac{(\max(f(m,n)))^2}{\frac{1}{N_f}\sum_{\forall(m,n)}(z(m,n)-f(m,n))^2}\right] \quad (7)$$

where f represents the original image, z indicates the stegoimage which the secret message is embedded, and N_f is the total number of pixels in the image. In this study, the number of entries in the palette has been set to 256 and the number of iteration for training palette is 60 times. The secret message is generated by a psudo random generator. The original cover image and stego image are both true color images.

Figs. 11 to 16 show two examples of the stego images. In Figs. 12 and 15, any pixel p is replaced by the centroid v_n of the cluster cn in which the pixel is classified or closest to it. If the value of a secret bit is the same as the assigned value of the node in MST, p will be replaced by the centroid v_A of the cluster c_A that it has been classified. On the contrary, p will be replaced with v_B of the cluster c_B which has the minimum distance to c_A. The number of colors in Figs. 12 and 15 is only 256. Although the PSNRs achieve 30.67dB and 29.97dB, respectively, for two images, the degradation of visual quality can be easily discriminated from the original secret image. The effect is even more obvious for Fig. 15 since it has more complex textures. Figs. 13 and 16 are stegoimages constructed using our proposed method, in which the PSNRs have been raised to 36.95dB and 35.86dB, respectively. The main improvement of our method is that p will attain its value if the value of a secret bit is the same as the assigned value of the node that p is classified, while it will be replaced with a pixel p' which is closest to it if the value of the secret bit is different from the assigned bit value of the corresponding node. In this case, the stegoimages are still be true color images that the number of colors is not altered that the visual quality is attained.

Table 2. Comparison of image quality (PSNR in dB) among various methods for Lena and Barb.

Image	Our method	EZ-stego	Fridrich
Lena	36.95	14.23	31.28
Barb	35.86	14.55	30.64

Recently, Wu et al. proposed a steganographic method by iterative calculated to obtain stegoimage with optimal palette [4], which greatly improved the method proposed by Fridrich [2]. It calculated the cost and benefit with the influence of embedding secret message before embedding, and adjusted coefficients in the palette according to cost and benefit until it reached the balance between cost and benefit. This method is effective in increasing the quality of steganography, and the result is batter then EZ stego [3] and Fridrich's method [2]. But the image quality of the stegoimages is limited by the number of colors in the palette. Two images shown in Fig. 17 were tested in their experiment. As demonstrated in Table 3, a comparison is made by calculating the PSNRs of the stego images obtained from various methods. As indicated in the table, it can be found that our method is better than the other three.

Table 3: Comparison of image quality (PSNR in dB) among various methods for Fruit and Swimmer.

	Proposed Method	**Wu et al.**	**EZ-Stego**	**Fridrich**
Fruit	34.09	31.48	23.67	28.48
Swimmer	36.58	35.87	21.68	25.98

(a) (b) (c)

Figure 11. (a) The original image of Lena and (b, c) displays of two enlarged local

(a) (b) (c)

Figure 12. (a) Stego image of Lena constructed by replacing a pixel with its closest color in the palette (PSNR=30.67) and (b, c) displays of two enlarged local areas.

(a) (b) (c)

Figure 13. (a) Stego image of Lena constructed by our proposed method (PSNR=36.95) and (b, c) displays of two enlarged local areas.

(a)

(b) (c)

Figure 14. (a) The original image of Barb and (b, c) displays of two enlarged local

(a)

(b) (c)

Figure 15. (a) Stego image of Barb constructed by replacing a pixel with its closest color in the palette (PSNR=29.77) and (b, c) displays of two enlarged local areas.

(a)

(b) (c)

Figure 16. (a) Stego image of Barb constructed by our proposed method (PSNR=35.86) and (b, c) displays of two enlarged local areas.

(a) (b)

Figure 17. Test images: (a) Fruit and (b) Swimmer.

4 Discussion and Conclusion

In the traditional methods, palette was utilized to implement steganography. The image quality of the stego image is usually limited by the number of colors in the palette. Although it significantly reduces the image size, it causes serious influence with regard to visual quality in loss of detail. The method proposed here also utilized palette, it does not limit the number of colors used in the stegoimage. The stegoimage still keeps the true-color form as the original cover image. The results show that the visual quality obtained by our proposed method is better than other traditional methods.

The disadvantages of the proposed method are listed as follows:

1. The cover image used for constructing the stegoimage might be slightly different from the image for decoding.
2. The ratio (bit per byte) of secret message to stegoimage size is reduced compared to the traditional method.

With regard to the first drawback, sometimes the cover original images used for hiding the secret message can be accessed from the internet, it is uncertain whether the receiver can get the same original image as the sender. If the receiver uses a slightly different cover image to extract the message from the received stegoimage, wrong message may be obtained.

For the second shortcoming, the experimental results demonstrate that the visual quality using our proposed method is better than the traditional methods. Although the hiding capacity is reduced in term of bit per byte, it still keeps the same capacity in term of bit per pixel. For example, if the number of colors of the palette is 256, it only needs 8 bits to represent a pixel for the stegoimage, but it needs 24 bits to represent a pixel in the stegoimage for our method.

In conclusion, we propose a steganography method which greatly improves the image quality compared to the traditional methods accompanied with an improvement in security and camouflage of the stegoimage by preventing the intruder's attention.

References

[1] C. L. Tsai, H. F. Chiang, K. C. Fan and C. D. Chung, Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism, *Pattern Recognition,* Vol.38, 2005, pp. 1993–2006

[2] J. Fridrich, A new steganographic method for palette-based images, *IS&T PICS, Savannah, Georgia 1999*, 1999, pp. 285–289.

[3] R. Machado. EZ Stego, Stego Online, Stego, Available from http://www.stego.com.

[4] M. Y. Wu, Y. K. Ho and J. H. Lee, An iterative method of palette-based image steganography. *Pattern Recognition Letters*, Vol.25, 2004, pp. 301-309.

[5] M. S. Shahreza, An improved method for steganography on mobile phone, *Proceedings of the 9th WSEAS International Conference on Systems*, 2005, pp. 1-3.

[6] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina , StegCure: a comprehensive steganographic tool using enhanced LSB scheme, *WSEAS Transactions on Computers,* Vol.7, Issue 8, 2008, pp. 1309-1318

[7] G. Brisbane, R. Safavi-Naini, and P. Ogunbona, High-capacity steganography using a shared colour palette, *Vision, Image and Signal Processing, IEE Proceedings*, Vol.152, Issue 6, 2005, pp.787-792.

[8] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath and S. Chandrasekaran, Robust Image-Adaptive Data Hiding Using Erasure and Error Correction, *IEEE Transactions on Image Processing*, Vol.13, Issue 12, 2004, pp. 1627-1639.

[9] R. Din , Hanizan Shaker Hussain , Salehuddin Shuib, The capability of image in hiding a secret message, *Proceedings of the 6th WSEAS International Conference on Signal, Speech and Image Processing*, 2006, pp.95-100.

[10] D. S. Yeung and X. Z. Wang, Improving Performance of Similarity-Based Clustering by Feature Weight Learning, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.24, Issue 4, 2002, pp. 556-561.

[11] X. H. Wang, Y. Wang and L. Wang, Improving fuzzy c-means clustering based on feature-weight learning, *Pattern Recognition Letters* Vol.25, Issue 10, 2004, pp. 1123-1132.

[12] S. Theodoridis and K. Koutroumbas, *Pattern Recognition 2nd. Ed.,* San Diego, CA: Academic Press, 2003.

[13] J. W. Han and M. Kamber, *Data Mining: Concepts and Techniques,* Morgan Kaufmann, 2000.

[14] T. Seppannen, K. Makela, and A. Keskinarkaus, Hiding information in color images using small color palettes, *Lecture Notes in Computer Science* , Vol.1975, 2000, pp. 69–81.

[15] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms 2nd Ed*., Massachusetts Institute of Technology, 2005.