

Chapter 5

Data Hiding in JPEG Image Mosaics and Its Application in Covert Communication

In this chapter, the tile images of an image mosaic are used to achieve a novel covert communication application in which high-resolution secret images can be transmitted. The idea of the proposed application originated with the puzzle game. Tile images here are regarded as the pieces of a puzzle, and after all the pieces are pieced together in a certain way, an image mosaic is presented. Furthermore, a new concept of double image authentication is also proposed to verify not only the fidelity and integrity of the cover image but those of the secret image.

The remainder of this chapter is organized as follows. Section 5.1 includes a review of related data hiding techniques and an introduction to the proposed application. Section 5.2 describes the proposed application and related works in detail. And finally some experimental results are shown, followed by some discussions in Section 5.3.

5.1 Introduction

Many researchers proposed different methods for covert communication via the Internet. Researchers in the cryptography field designed methods in terms of encryption techniques. Communication security is guaranteed by such methods because trying out all ways to decrypt the secret is time-consuming and complicated

in computation. However, the encrypted media are not convenient for uses in many application conditions, and their appearances can often be distinguished from those of other media easily, arousing the curiosity of illegal users. On the other hand, data hiding techniques are applied to hide information in digital images to achieve the effect of covert communication. Most of them embed text files in images because the hiding capacity of an image is usually not very large. Unlike the cryptography approach, the cover image can be used in public without causing suspicion and only legal users, who know the steganography hint, can extract data from it.

Image mosaics are new media for use in covert communication. In view of its properties to the human visual system, tile images are used for hiding data in the proposed covert communication application. The idea of the proposed application comes from the concept of puzzle game, regarding tile images as the pieces of a puzzle. All pieces of the puzzle are composed to generate an image mosaic as the result of a puzzle game. In the proposed application, a secret image is divided into parts as secret pieces and the data hiding technique is then applied. The resolution of a secret image used in the proposed application relies on the resolution of an image mosaic. Generally speaking, the more tile images the image mosaic contains, the higher resolution a secret image can be. Additionally, after considering that people might modify the cover image and so alter the secret image which is part of the cover image, a concept of double authentication is proposed to verify not only the cover image but also the secret image.

In this study, images with the JPEG format are used. Some related data hiding techniques and image authentication methods are reviewed in advance.

5.1.1 Review of DCT-Domain Data Hiding

Images compressed by the JPEG standard are called JPEG images. The JPEG compression process includes four steps. The source image is first divided into several non-overlapping 8×8 blocks. Then 8×8 forward discrete cosine transform (FDCT) is applied to each block to produce 64 integer values, called DCT coefficients. The DCT coefficients are quantized by a standard quantization table as shown in Table 5.1. Finally entropy coding is used to remove the coding redundancy existing in the DCT coefficients. Figure 5.1 shows a flowchart of the JPEG compression process and Figure 5.2 shows a flowchart of the JPEG decompression process.

Several researchers investigated how to hide data in images with the JPEG format. Yin and Tsai [13] proposed a DCT-based method to embed annotations in JPEG images by adjusting the magnitude relation of two DCT coefficients. These two DCT coefficients, denoted as S_1 and S_2 , are located in at coordinates (1, 4) and (2, 3) of the standard quantization table within an 8×8 block. The embedding rules for a bit b of the annotation data are described as follows:

1. if b is “1” and $S_1 < S_2$, then exchange S_1 and S_2 ;
2. if b is “0” and $S_1 \geq S_2$, then exchange S_1 and S_2 ;
3. for other cases, leave S_1 and S_2 unchanged.

Then, a bit b is extracted from a 8×8 block according to the following rules:

1. if $S_1 \geq S_2$, then a bit “1” is extracted;
2. if $S_2 \geq S_1$, then a bit “0” is extracted.

The annotation data can be reconstructed after extracting all the data embedded in each 8×8 block.

Yin and Tsai [13] also proposed a method to embed authentication signals in JPEG images. The authentication signals are embedded into locations in the high frequency part of the DCT coefficients. The image can be verified by checking the embedded fragile authentication signals to see whether they are destroyed or not.

Table 5.1 A standard quantization table in the JPEG compression standard (luminance component).

(u,v)	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

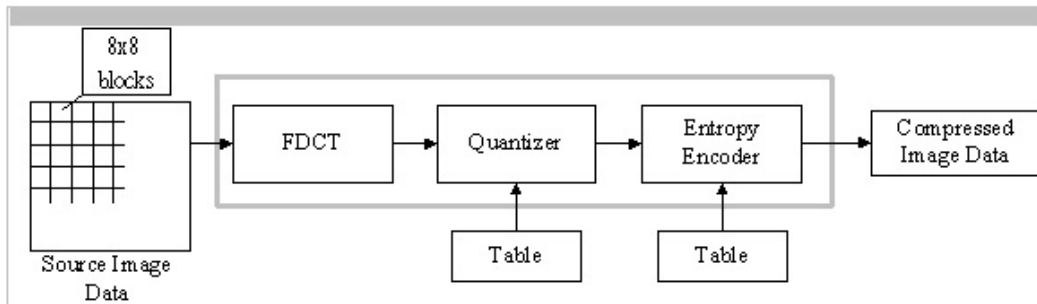


Figure 5.1 DCT-Based Encoder Processing Steps.

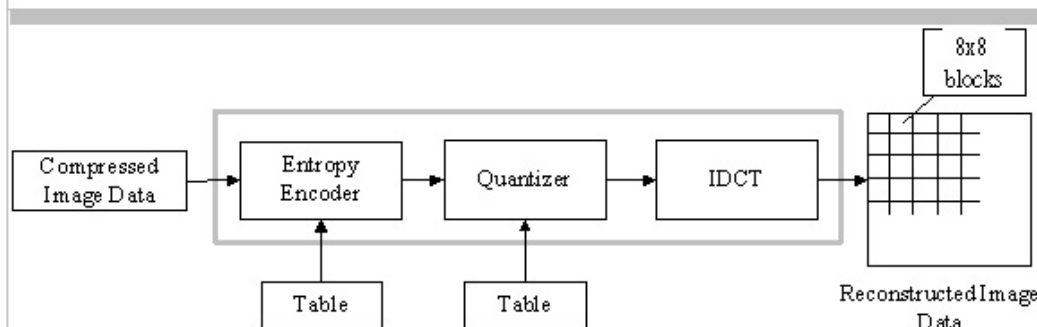


Figure 5.2 DCT-Based Decoder Processing Steps.

5.1.2 Problem Definition

Recall the image mosaic creation process, in which an image database is organized prior to the creation process. As a result, a secret image database organization process is required in the proposed method in order to build a mosaic composed of a secret image. For later secret image recovery and authentication purposes, the data hiding technique in the DCT-domain is applied while organizing the database. And authentication signals are generated and embedded in the mosaic during the mosaic creation stage. Because the locations of the selected coefficient pair for different purposes are different, how to integrate these selected coefficient pairs for the embedding process and how to distinguish them from different purposes by the embedded data during the extracting process are important in this application.

5.2 Proposed Application of Mosaic Images in Covert Communication

5.2.1 Application Overview

The proposed application is based on the idea of puzzle game. Tile images, are regarded as the pieces of a large puzzle, which can be pieced together to result in an image mosaic. On the other hand, a secret image is regarded another small puzzle image in this application. It is divided to generate fractional pieces of the small puzzle image. And the *division signals* are generated and embedded right in the fractional pieces in the meantime. The original secret image can be reconstructed by reconstructing all the fractional pieces according to the embedded division signals. It means that the embedded division signals will be of help for secret image recovery.

So the division signals must be strong enough to avoid tampering because the mosaic with the JPEG format may suffer from a re-compression attack frequently. On the other hand, authentication signals are also embedded in each piece of the secret image in this study for the purpose of authenticating the recovered image. The authentication signals are fragile in order to detect the slight changes of the image.

During the process of image mosaic creation, a header should be embedded in certain tile images that are not any pieces of the secret image. The header gives an instruction to distinguish the pieces of the puzzle for the data extraction process. And certain other types of authentication signals are generated and embedded in all tile images to verify the integrity and fidelity of the cover image. Figure 5.3 shows a diagram of the proposed covert communication application and Figure 5.4 shows a flowchart of the proposed embedding process of the application.

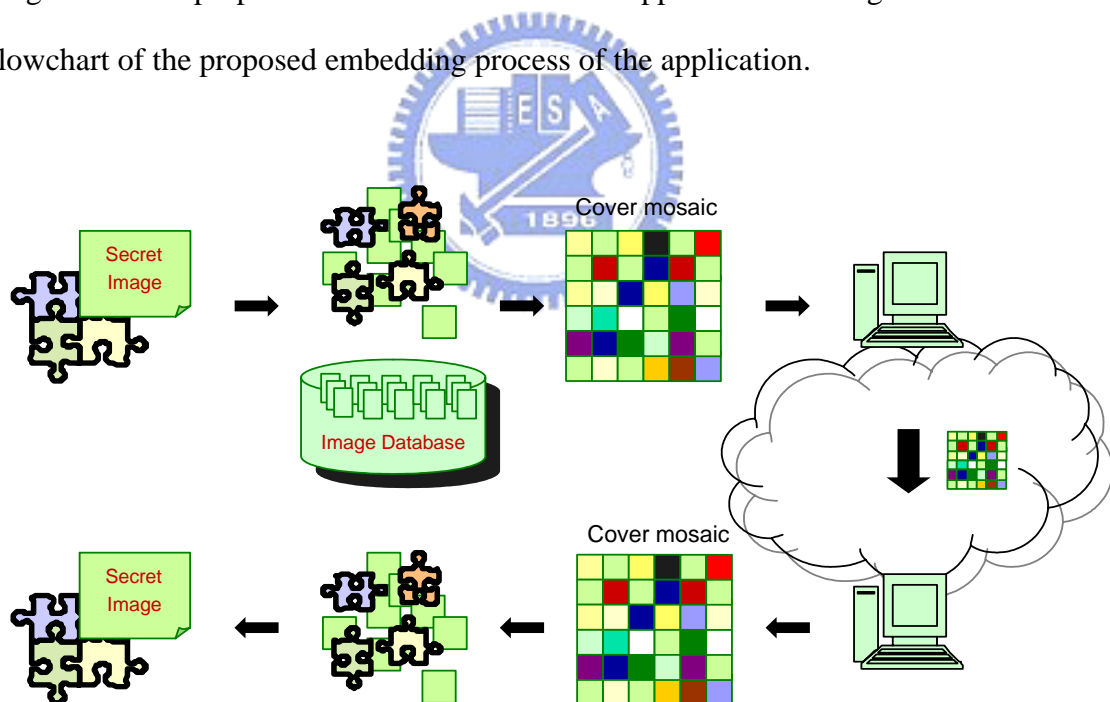


Figure 5.3 Diagram of the covert communication application.

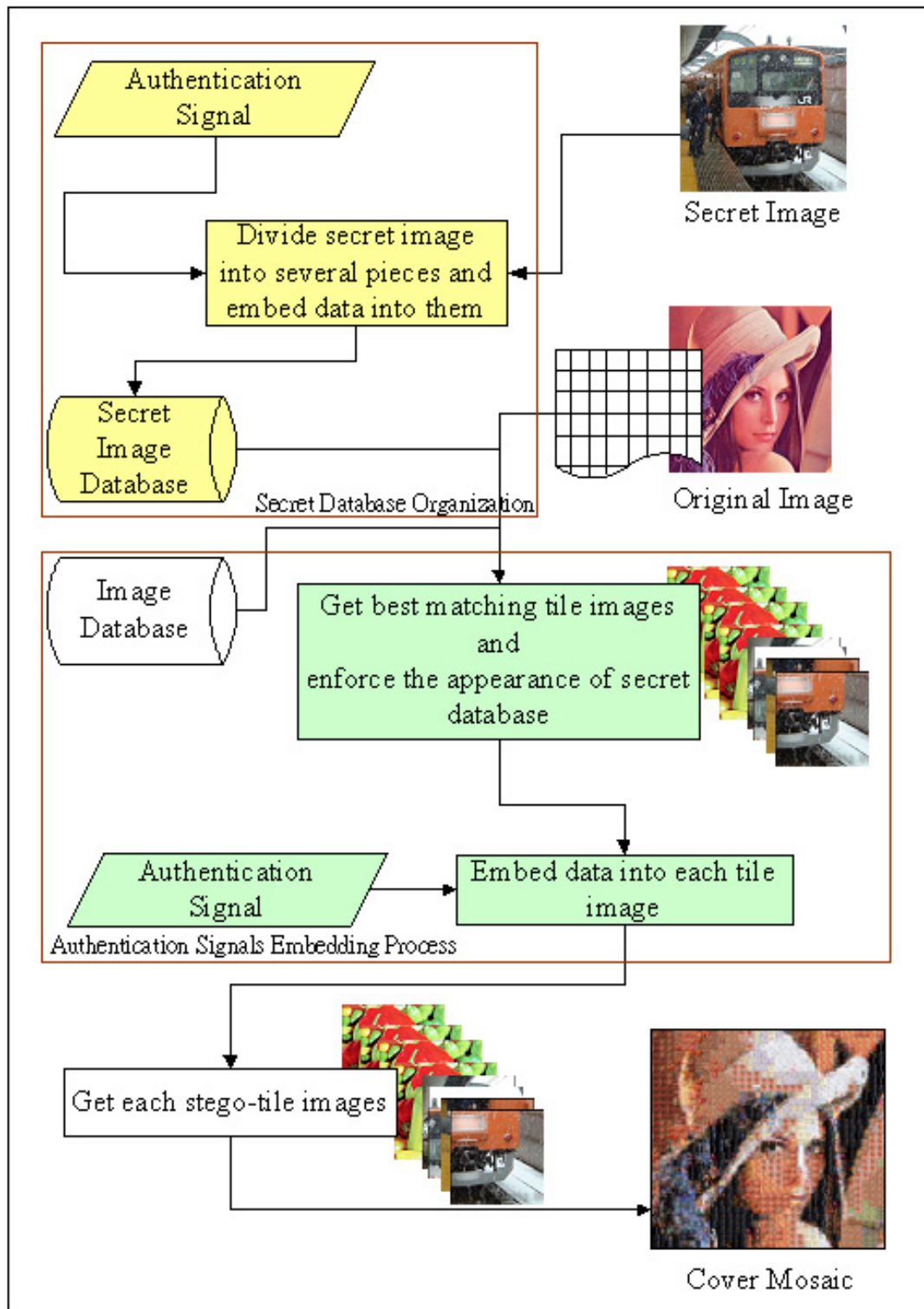


Figure 5.4 Flowchart of proposed covert communication application.

5.2.2 Secret Image Database Organization

The secret image database organization process includes three main parts. A secret image is first divided into pieces and then the previously-mentioned data hiding technique is applied to embed relevant division signals in each piece. Additionally, the previously-mentioned authentication signals are also embedded for the image authentication purpose. And a secret image database is organized finally according to Algorithm 2.2. The following sections will describe the details about these three major steps and Figure 5.5 illustrates a flowchart of the secret image database organization process.

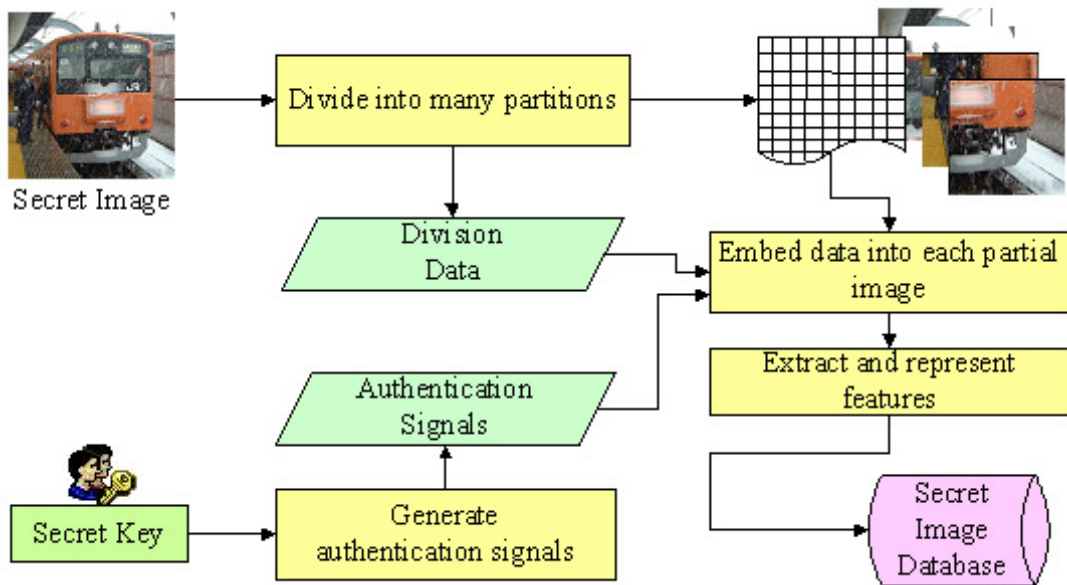


Figure 5.5 Flowchart of the secret image database organization process.

A. Secret Image Division

In the secret image division process, the size of each piece is defined according to the setup of the original tile size in the mosaic creation process. We make two assumptions to avoid certain division problems. Firstly, the width and height of the secret image are assumed to be multiples of the width and height of the tile image, respectively, and secondly a secret image must be bigger than a tile image. In this way,

the size of each piece of the secret image could be the same as those of the tile images in the image database. The division signals are generated simultaneously when the secret image is divided into pieces.

B. Division Signal Embedding Process

A division signal is embedded into an image for recording the information of how a secret image is divided. The number of the division signals equals the number of the divisions of the secret image. Each division signal includes 12 bits of the coordinate information and 4 bits of the header information. The coordinate information is the record of the x and y coordinates of the current piece within the secret image. So far, 6 bits of the coordinate information are represented as the x coordinate such that the maximum is 64 in a decimal system. So does the y coordinate which has the maximum of 64. We assume that the minimum size of a tile image is 32×32 which has sixteen 8×8 DCT blocks, and so the maximum size of a secret image that can be covered is 2048×2048 which yields the maximum capacity of the covert communication application. 4-bit headers are used to distinguish secret pieces from normal tiles. The header is important for the extraction process; otherwise, the secret image recovery process will fail. Table 3.2 shows the structure of a 16-bit division signal.

Table 5.2 Information in a division signal with 16 bits length.

4 bits header	6 bits x coordinate information	6 bits y coordinate information
---------------	-----------------------------------	-----------------------------------

For the reasons of the robustness of the hidden data, two DCT coefficients located at (0,5) and (3,2) of the standard quantization table are chosen for the embedding process. The embedding rules are listed as follows.

Algorithm 5.1: DCT-domain Embedding Rule.

Input: the selected pair C_1 and C_2 of coefficients in an 8×8 DCT block, an stream S to be embedded, and a threshold T .

Output: an 8×8 DCT block B .

Steps.

Step 1. Compute the absolute difference D between C_1 and C_2 :

$$D = |C_1 - C_2|$$

Step 2. Adjust the relations between C_1 and C_2 by the following rules where M_1 is the average of C_1 and C_2 .

A. If $D \leq T$:

$$\begin{cases} \text{if } S \text{ is odd, then set } C_1 > C_2 \text{ and } |C_1 - C_2| = T_3; \\ \text{if } S \text{ is even, then set } C_2 > C_1 \text{ and } |C_1 - C_2| = T_3. \end{cases}$$

B. If $D > T$:

$$\begin{cases} \text{if } S \text{ is odd and } C_1 < C_2, \text{ then set } C_1 = M_1 + (T_3 / 2) \text{ and } C_2 = M_1 - (T_3 / 2); \\ \text{if } S \text{ is even and } C_2 < C_1, \text{ then set } C_1 = M_1 - (T_3 / 2) \text{ and } C_2 = M_1 + (T_3 / 2). \end{cases}$$

The threshold T is used to increase the robustness of the hiding method.

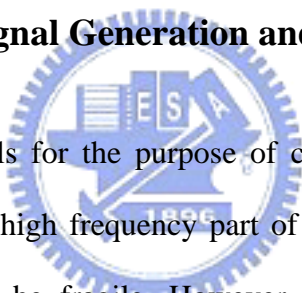
C. Authentication Signals Generation and Embedding Process

Authentication signals are used for the image authentication purpose. They are embedded in the high frequency part of the DCT coefficients. In this study, authentication signals are generated with 8 bits by the operations of a secret key and the coordinate information that is described in the previous section. Three pairs that are located at (5, 3) and (3, 6), (6, 3) and (4, 5), and (6, 2) and (4, 4) in the standard quantization table in Table 5.1 are chosen to embed the authentication signals. The embedding rules are the same as *Algorithm 5.1*.

5.2.3 Cover Mosaic Creation Process

Three main tasks are dealt with in the cover image mosaic creation process. Consider the similarity measure of the mosaic creation process. A tile image is selected if it has the smallest distance to the corresponding target image. However, in this application, the pieces of the secret image must appear at least once so that they can finally be integrated as the original secret image. The methods that are described in Chapter 2 to enforce the appearances of tile images are used here. On the other hand, a 4-bit header information and authentication signals are embedded into the cover image. We will describe the details in the following.

A. Authentication Signal Generation and Embedding Process



The authentication signals for the purpose of cover mosaic authentication are embedded at locations in the high frequency part of the standard quantization table because they are allowed to be fragile. However, the chosen locations must be different from those that have been chosen for other purposes before. Similarly, the authentication signals are generated with use of a secret key and certain embedding coordinates. Three pairs are chosen for embedding the authentication signals and they are located at the coordinate pairs of (5,3) and (3,6), (6,3) and (4,5), and (6,2) and (4,4) in the standard quantization table.

B. Header Information Embedding Process

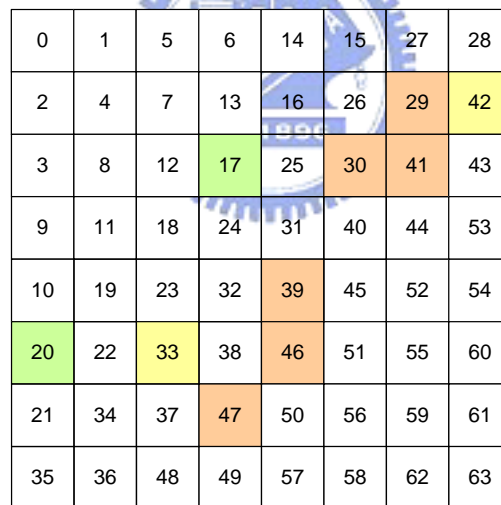
The header information described previously is a 4-bit binary number. It is embedded in each tile image that is selected from a normal image database rather than from the secret image database. The first bit of the header is set to be “1” and used to

express the attribute of tile image. The other three bits of the header may be preserved for other purposes or applications, for example, to indicate the integration with a certain other data hiding method that we will not mention in this study. The locations of a selected pair in the standard quantization table for embedding the header are the same as those for embedding the division signals which are located at (0,5) and (3,2). Table 5.3 shows the structure of the 4-bit header.

Table 5.3 The structure of a 4-bit header.

1	0	0	0
---	---	---	---

All locations used for hiding data in the standard quantization table in this application are illustrated in Figure 5.6.



0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Figure 5.6 Locations for different purposes in the standard quantization table.

Locations at 17 and 20 are used for embedding location data. Locations at 29, 30, 41, 39, 41, 46, and 47 are used for embedding authentication signals of the secret image. Locations at 33 and 42 are used for embedding authentication signals of the cover mosaic.

5.2.4 Mosaic Images Authentication Process

Because the proposed authentication process is a tile-based method, the tile size detection process that was described in Chapter 3 is first applied to the mosaic. Then the embedded authentication signals are extracted according to the following data extraction method.

Algorithm 5.2: Data extraction method.

Input: an 8×8 DCT block, and a coefficient pair (C_1, C_2) of an 8×8 DCT block.

Output: an extracted bit S .

Steps.

Step1. Extract an embedded bit by the following rule:

$$\begin{cases} \text{if } C_1 > C_2, \text{ take } S \text{ to be "0"}; \\ \text{if } C_1 < C_2, \text{ take } S \text{ to be "1"}. \end{cases}$$

The extracted authentication signals are verified by comparing them with the other authentication signals which are generated by the use of a correct key and the location of the 8×8 DCT block. 8×8 DCT blocks are verified based on the following algorithm and Figure 5.7 shows a flowchart of the mosaic authentication process.

Algorithm 5.3: Verification of an 8×8 DCT block.

Input: a bit of the extracted signal S_1 , and a bit of the generated signal S_2 .

Output: a verification description.

Steps.

Step 1. Verify the input bit according to the following rule:

$$\begin{cases} \text{if } S_1 = S_2, \text{ then label this block as unauthentic}; \\ \text{if } S_1 \neq S_2, \text{ then label this block as unauthentic}. \end{cases}$$

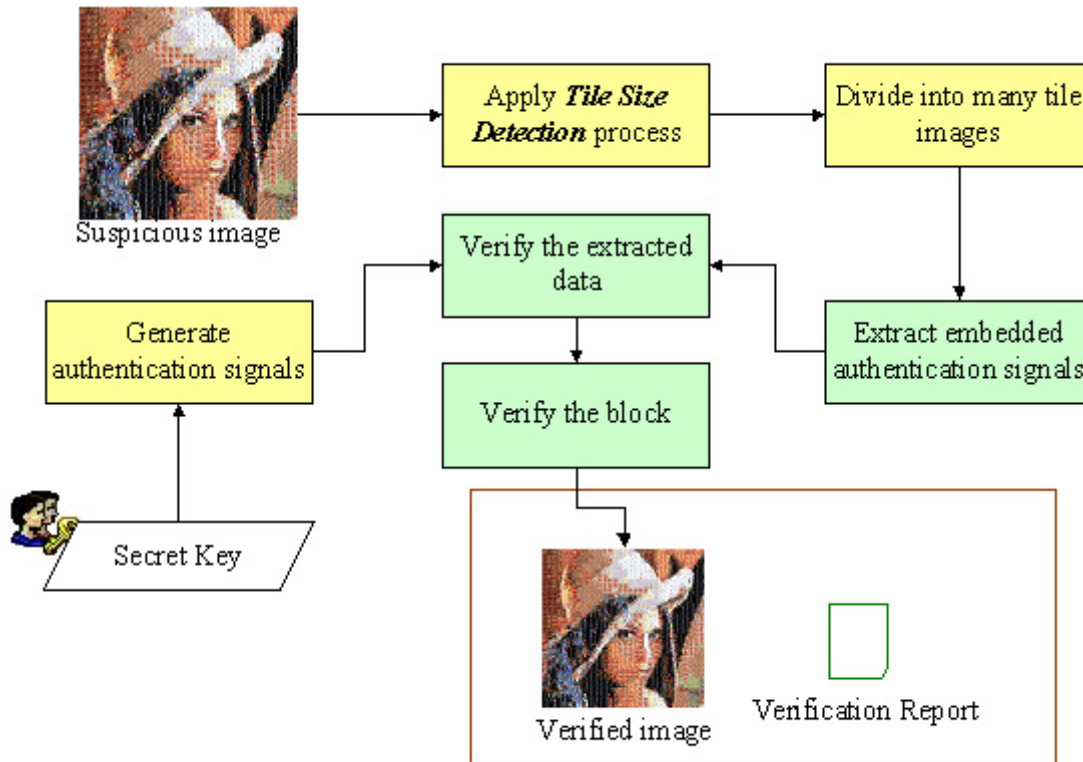


Figure 5.7 Flowchart of proposed image mosaic authentication process.

5.2.5 Secret Image Recovery Process

The secret image recovery process includes three stages. Above all, the pieces of the secret image are determined by the extracted header information from the pieces of the mosaic. And the secret image recovery process is applied after the location information is extracted from the pieces of the secret image. Furthermore, image authentication is necessary for the secret image to verify its fidelity and integrity.

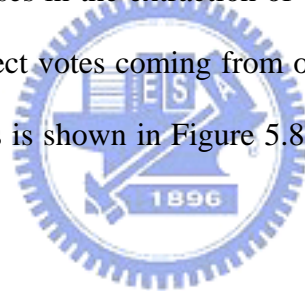
A. Location Data Extraction Process

The embedded bits are extracted from each secret piece by means of *Algorithm 5.2*. And the x and y coordinate information of a secret piece is derived by combining these extracted bits according to Table 5.2. After extracting all of the location data

from the secret pieces of the mosaic, the proposed secret image recovery process is applied to compose them together.

B. Secret Image Recovery Process

With the extracted location data of each piece of the secret image, it is easier to conduct secret image recovery. Because each piece of the secret image is to be used at least once while building the image mosaic, it is hard to just get the number of pieces for secret image recovery. Instead of discarding the duplicate pieces, a voting scheme comes into use for the voting of the most correct piece of the secret image. Moreover, the voting method of the recovery process will also contribute the best recovery result because the seldom failure cases in the extraction of the location data can be ignored by the dominance of the correct votes coming from others pieces. A flowchart of the secret image recovery process is shown in Figure 5.8, and a corresponding algorithm is described as follows.



Algorithm 5.4: Secret Image Recovery Process.

Input: a cover mosaic M and a secret key K .

Output: a secret image S .

Steps.

Step1. Derive the tile size by applying *Algorithm 3.2*.

Step2. Apply *Algorithm 5.2* to extract the embedded header information located at (0,5) and (3,2) in each 8×8 DCT block of a tile image.

Step3. Extract the embedded location data L located at (0,5) and (3,2) in each 8×8 DCT block of a tile image according to the extracted header information and label the tile image as a piece of the secret image if L is "0."

Step4. Get all pieces of the secret image and their location data.

Step5. Vote for the correct pieces by grouping all pieces at the same location.

Step6. Compose pieces obtained in Step 5 to recover the secret image.

C. Secret Image Authentication Process

In this study, we propose the concept of authenticating both of the secret image and the cover image. The stego-image may proportionally suffer from some malicious changes, such as replacing or adding features while transmitted to the receiver. Because the secret image in the form of pieces is part of the stego-image, it is desired to authenticate the stego-image to prevent the occurrence of the case that the secret image is changed. This case may happen under the assumption that the algorithm of constructing the stego-image is publicized. On the other hand, a receiver by far does not know what the secret image is indeed. Therefore secret image authentication is also required to provide the integrity information of the extracted secret image.

A flowchart of the authentication process is shown in Figure 5.8. A voting scheme is used for reducing the failure of the extraction process. Then the recovered secret image can be verified by the embedded authentication signals.

5.3 Experimental Results and Summary

Here we give two experimental results of the proposed covert communication and one experimental result of image authentication.

Figure 5.9 shows an original image and a secret image of a covert communication session, and two kinds of cover mosaics are shown in Figures 5.10 and 5.11, respectively. One is built by the use of both the secret image and the normal databases, the other only by the use of the secret image as a database. Figure 5.12

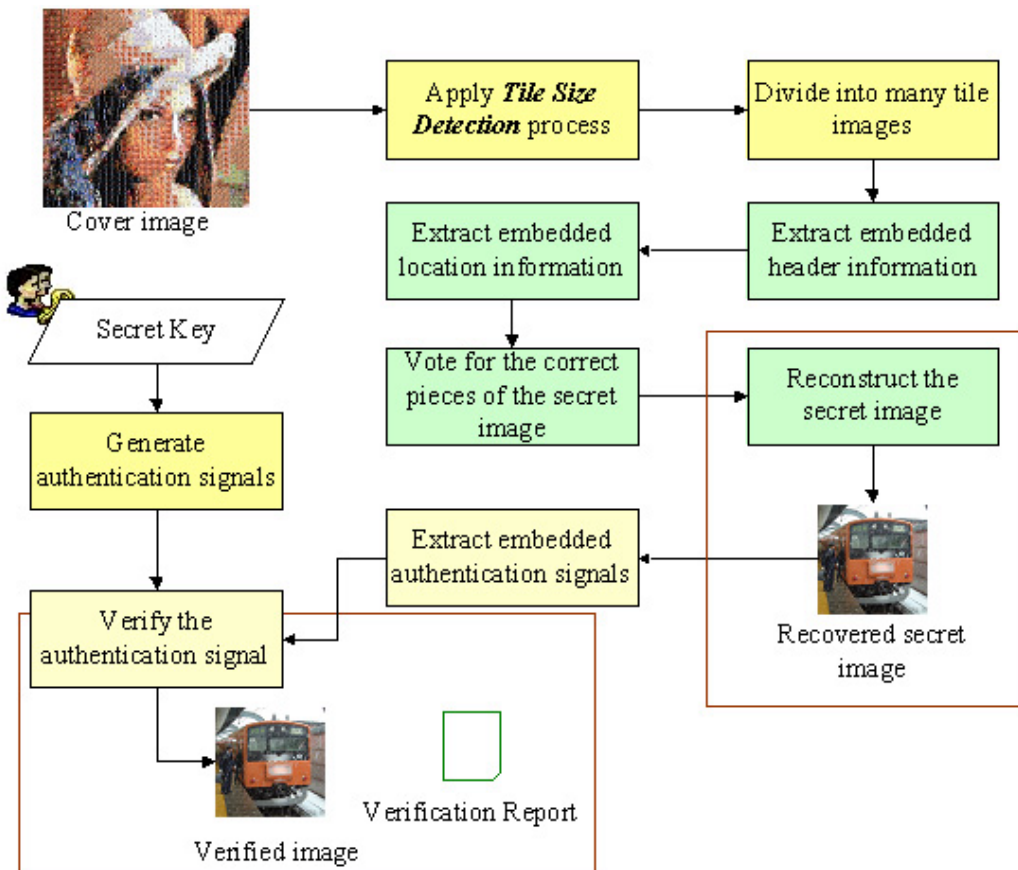


Figure 5.8 Flowchart of secret image recovery and authentication process.

shows the recovered secret image and the results of the image authentication on both the cover mosaic and the secret image are shown in Figure 5.13. The other experimental result is shown in Figure 5.14 through Figure 5.16.

The concept of putting the secret image within the mosaic seems just like the concept of cryptography because they both protect the media from tampering by time complexity. Attackers may also use an exhaustive searching method for composing the secret image from the cover mosaic, but it is time-consuming and computation-intensive. We may enlarge the cover mosaic size and downscale the tile size to increase the complexity of searching to prevent it from tampering.



(1)



(2)

Figure 5.9 The original image and the secret image. (1) The original image for covert communication. (2) The secret image (256×256).

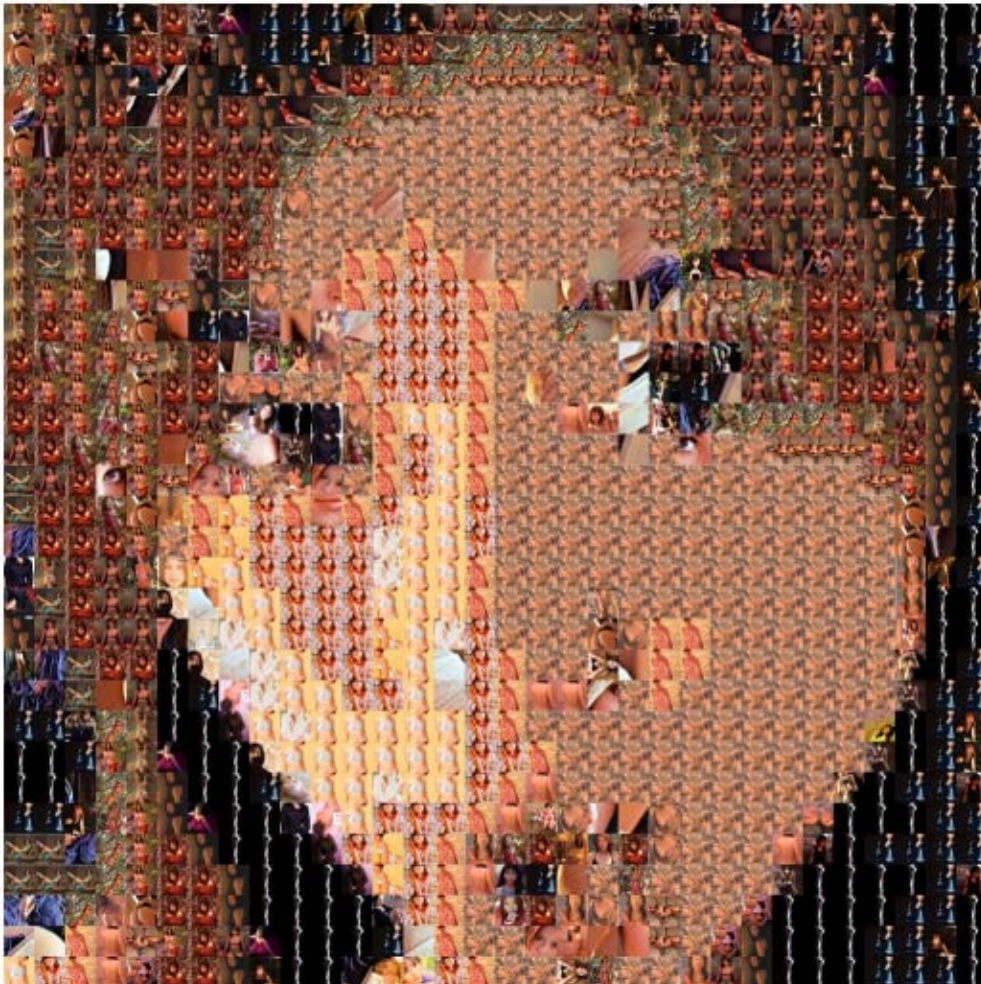


Figure 5.10 The cover mosaic (1024×1024) with 1024 tiles (32×32). The secret image is divided into many tile images and is integrated with other tile images in a certain way to yield a cover mosaic.

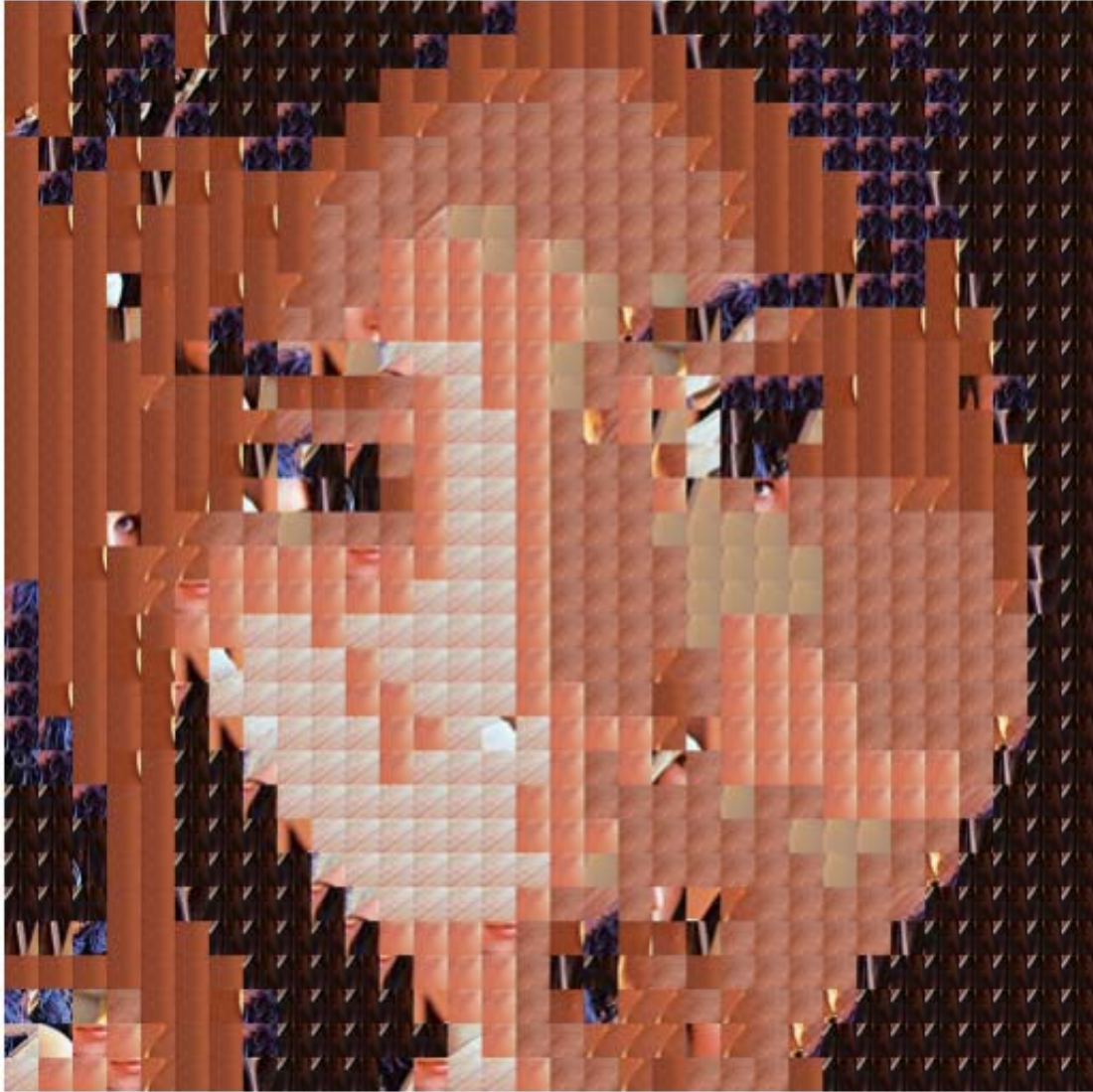


Figure 5.11 The cover mosaic (1024×1024) with 1024 tiles (32×32). The secret image is divided into many tile images and is used as a database to produce the cover-mosaic.



Figure 5.12 The recovered secret image. (PSNR=29.8)

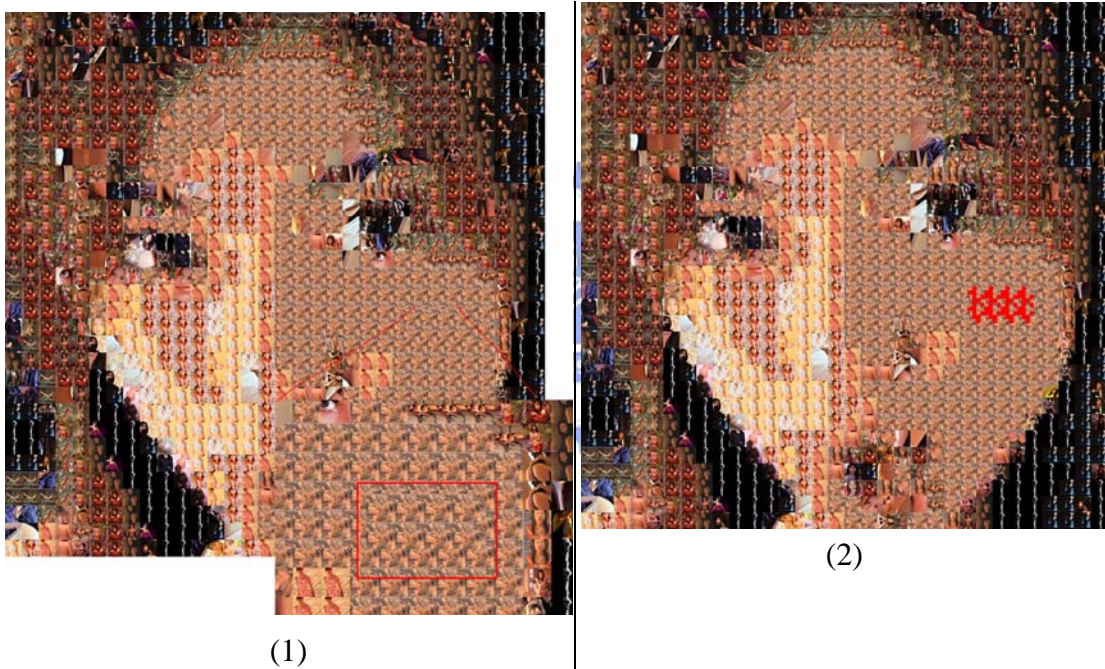


Figure 5.13 The authentication of the image mosaic. The mosaic in (1) is tampered with the replacement of the region nearby and the red region of (2) shows the authentication result. (1) The mosaic is tampered with the replacement of the region. (2) The verified mosaic.



(1)



(2)

Figure 5.14 The original image and the secret image. (1) The original image for covert communication. (2) The secret image (256×256).

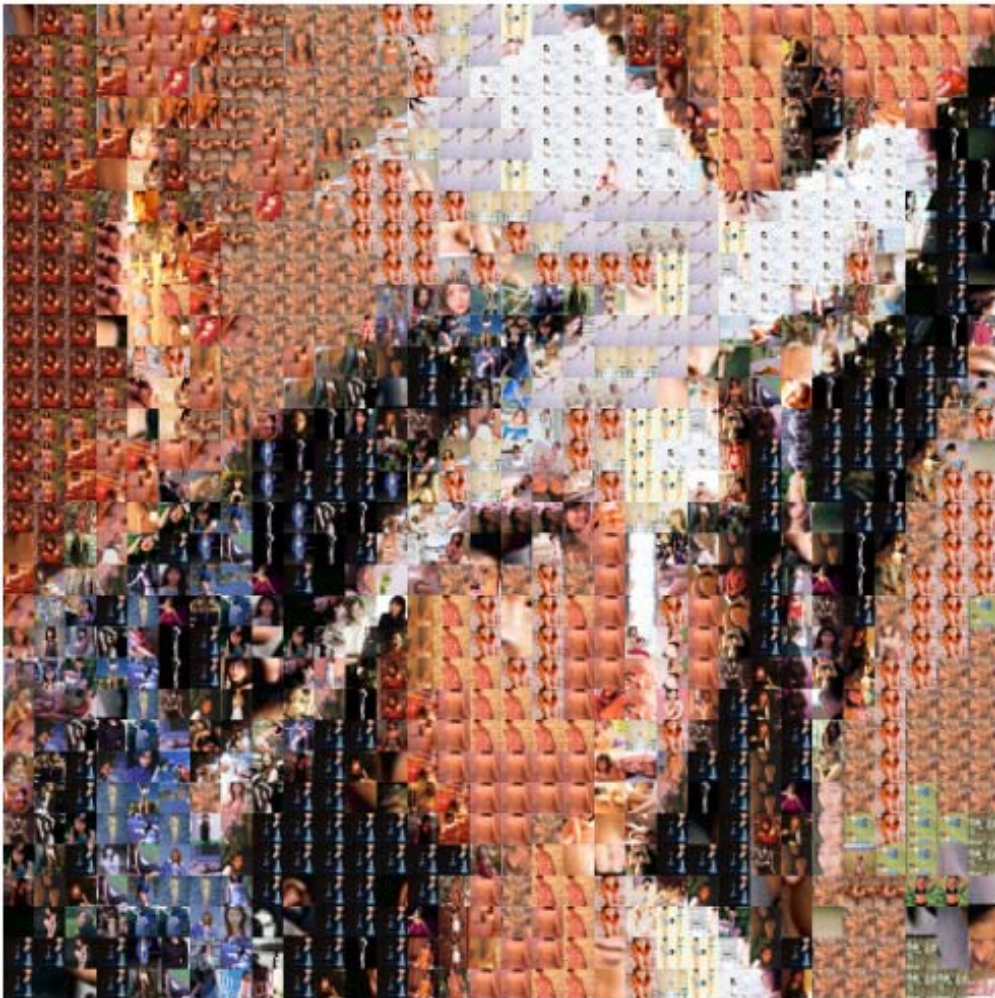


Figure 5.15 The cover mosaic (1024×1024) with 1024 tiles (32×32). The secret image is divided into many tile images and is used as a database to produce the cover-mosaic.



Figure 5.16 The recovered secret image. (PSNR=34)



Chapter 6

Conclusions and Suggestions for Future Works

6.1 Conclusions

In this study, we first built a system for image mosaics creation. The system includes the functional modules of image database construction, image feature extraction, similarity measurement, and tile arrangement. And three methods have been proposed for use in the system. In view of producing image mosaics of different styles, the first proposed method has the capability of forming tiles with dots or hexagonal shapes by the use of different weighted average matrices, different tile arrangements, and different shape properties. The second proposed method place top priority on selected images to achieve the enforcement of their appearances. And the third proposed method modifies the color distribution of an image slightly in the HSI color model to create an image mosaic that is more similar to the original image.

Image mosaics may be shown in various media, such as being displayed by a computer, or being printed as posters or artistic productions. In order to protect the copyright of image mosaics, a method based on the concept of image coding has been proposed. The method takes advantage of the property of image mosaic in the human visual system to embed a semi-visible watermark by adding visible boundary regions. The embedded semi-visible watermark both can be extracted from the mosaic with the digital form and can be detected after the mosaic goes through a print-and-scan process. Furthermore, three methods of tile size detection, tilt detection, and border

detection have been proposed by use of the techniques of edge detection and projection for the purposes of facilitating the watermark extraction process against print-and-scan attacks.

Next, a novel data hiding method based on the histogram modification in the spatial domain by use of the hue component in the HSI color model has been proposed. The embeddable pixels are determined first in each 8×8 block by comparison of the hue values. Authentication signals are embedded into embeddable pixels pixel by pixel, block by block, and tile by tile by adjusting their hue values. Then the embedded data can be extracted by comparing the hue value with the maximum bin peak of the block in the hue channel. As a result, the mosaic can be verified to check its integrity and fidelity.

Finally, a method using the tile images of an image mosaic to achieve a novel covert communication application has been proposed, which can be used to transfer a higher resolution secret image. The idea of the proposed application originated with the puzzle game. A secret image is divided into many tile images for use in the mosaic creation process. And the secret image can be recovered according to the extracted division signals embedded in the image. Furthermore, a concept of double image authentication and a corresponding method to verify not only the fidelity and integrity of the cover image but of the secret image has been proposed. Because the cover-mosaic might proportionally suffer from malicious changes, such as replacing or adding features, these changes should not disturb the secret image within the mosaic. And the proposed method can be used to verify this requirement.

6.2 Suggestions for Future Works

In this study, we have proposed some methods for image mosaics creation,

copyright protection, image mosaic authentication, and covert communication. However, there are still some interesting topics for image mosaic creation and data hiding in image mosaics which are worth for further study. They are listed as follows:

1. Extending the proposed method of image mosaic creation for imitating the style of other artistic works.
2. Producing image mosaics with irregular forms of shapes based on computer graphics.
3. Blurring the bad impression effects of the discontinued seams between two adjacent tile images by high-pass or gaussian filters in the frequency domain.
4. Designing practicable methods to quantize and evaluate the impression quality of created image mosaics.
5. Designing more efficient tile arrangement methods.
6. Optimizing the image mosaics created with databases with only limited numbers of images.
7. Studying algorithms to find a set of images that are used most frequently in image mosaic creation.
8. Combining the three proposed data hiding methods and applying them to an image mosaic in order to have the more strong capability.
9. Keeping the image quality good after embedding a large amount of data.
10. Applying created image mosaics to more aspects of human daily life.

References

- [1] R. Silvers, and M. Hawley, *Photomosaics*, Henry Holt and Co., 1997.
- [2] C. Close, and J. Yau, *Recent Paintings*, Pac Wildenstein, 1995.
- [3] S. Dali. *The Salvador Dali Museum Collection*, Bulfinch Press, 1996.
- [4] L. Harmon. "The Recognition of Faces," *Science American*, No. 5, November, 1973, pp. 70-82.
- [5] R. Silvers. Photomosaic, <http://www.photomosaic.com>, 1996.
- [6] R. Silvers. "Digital Composition of a Mosaic Image," US Patent and Trademark Office. <http://www.uspto.gov>. No. 957833. October.2000.
- [7] A. Finkelstein, and M. Range. "Image Mosaics," *Technical Report: TR-574-98*, Computer Science Department, Princeton University, Princeton, U.S.A., 1998.
- [8] N. Tran. "Generating Photomosaics: An Empirical Study," *Proc. ACM Symposium on Applied computing (SAC '99)*, San Antonio, Texas, U.S.A., 1999, pp. 105-109.
- [9] Y. Zhang, M. A. Nascimento, and O. R. Zaiane, "Building Image Mosaics: An Application of Content-Based Image Retrieval," *Proc. IEEE Int. Conf. On Multimedia and Expo (ICME' 03)*, Baltimore, U.S.A., July, 2003.
- [10] C. Blundo, and C. Galdi, "Hiding Information in Image Mosaics," *The Computer Journal*, vol.46, issue 2, Feb.2003, pp.202-212.
- [11] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *Proc. IEEE Int. On Circuits and Systems (ISCAS'03)*, Vol. 2, Bangkok, Thailand, May 25-28, 2003. pp.912-915.
- [12] Y. J. Cheng, "Copyright and Integrity Protection for Images by Removable Visible Watermarking Techniques," *M. S. Thesis*, Department of Computer and

Information Science, National Chiao Tung University, Hsinchu, Taiwan, June 2002.

- [13] C. Y. Yin, "Copyright and annotation protection in digital museums by using data hiding, watermarking, and image authentication techniques," *M. S. Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, June 2001.
- [14] C. H. Tzeng and W. H. Tsai, "A New Approach to Authentication of Binary Images for Multimedia Communication With Distortion Reduction and Security Enhancement," *IEEE Communications Letters*, Vol. 7, No.9, September 2003.
- [15] J. Fridrich, "Image Watermarking for Tamper Detection", *Proc. IEEE Int. (ICIP '98)*, Vol. 2, Chicago, U.S, 4-7 Oct. 1998, pp.404-408.
- [16] R. Ulichney, "*Digital halftoning*", MIT Press, Cambridge, Massachusetts, 1987.
- [17] W. L. Hunt, "*The Theory of PhotoTiled Pictures*",
<http://home.earthlink.net/~wlhunt/Theory/Theory.html>, 1998.
- [18] W. Niblack, R. Barber, W. Equitz, M. Flickner, E. Glasman, D. Petkovic, P. Yanker, C. Faloutsos and G. Taubin. The QBIC Project: Querying Images by Content Using Color, Texture, and Shape. In *Storage and Retrieval for Image and Video Databases*, SPIE, 1993, pp.173-187.
- [19] C. Carson, V. E. Ogle, "Storage and Retrieval of Feature Data for a Very Large Online Image Collection", *IEEE Data Engineering Bulletin*. Vol. 19, Vol. 4, December 1996, pp.19-27.
- [20] W. Hsu, T. S. Chua and H. K. Pung, "An Integrated Color-Spatial Approach to Content-based Image Retrieval", *Proc. ACM Multimedia '95*, Sam Fancisco, Nov 1995, pp.305-313.
- [21] C. Gonzalez and E. Woods, "*Digital Image Processing 2nd Edition*", ISBN.0-13-094650-8, pp.289-302.