Global Journal of Engineering Science and Research Management

A NEW SECURE VIDEO TRANSMISSION TECHNIQUE ON FRAGMENTED MOSAIC FRAMES

Jinu Xavier[*1], Leya Elizabeth Sunny[2]
[*1]Computer Science Department, KMEA Engineering College, India.
[2]Computer Science Department, KMEA Engineering College, India.

KEYWORDS: mosaic frames, Color transformations, pseudorandom number generated key, loseless data hiding.

ABSTRACT
A new secure video transmission technique is proposed which transforms the frames of the secret video into a so called secret fragment visible mosaic frames of the same size. The mosaic frame which looks similar to an arbitrarily selected target video frame and may be used as a camouflage of the secret frame, is yielded by dividing the secret frame into fragments and transforming their color characteristics to be those of the corresponding blocks of the target frame. Skillful techniques are designed to conduct the color transformation process and also suitable rotations of the mosaic frame is done so that the secret image may be recovered nearly losslessly and target image looks like original one. A scheme of handling the overflows/underflows in the converted pixels color values by recording the color differences in the untransformed color space is also proposed. Moreover the embedding details, rotation details and color transformation details will be shuffled with a pseudo random number using a key value in such a way that only the intended recipient who has the key will be able to retrieve back the secret data from the cover video without any distortion to both. This can be considered as a lossless data hiding method and a secured one.

INTRODUCTION
At present, images from different sources are often used and transmitted through the web for different applications, for example, online individual photo collections, private venture files, archive stockpiling frameworks, medicinal imaging frameworks, and military image databases. These images normally contain private or classified data so that they ought to be shielded from spillages amid transmissions. As of late, numerous routines have been proposed for securing image transmission, for which two basic methodologies are image encryption and data hiding.

Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties [1]–[7]. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding [8]–[10] that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this paper is an image. Existing data hiding methods mainly utilize the techniques of LSB substitution [8], histogram shifting [9], difference expansion [10]–[11], prediction-error expansion [12]–[13], recursive histogram modification , and discrete cosine/wavelet transformations.

However, in order to reduce the distortion of the resulting image, an upper bound for the distortion value is usually set on the payload of the cover image. A discussion on this rate distortion issue can be found in [19]. Thus, a main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical.

Moreover, most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts

Global Journal of Engineering Science and Research Management

OVERVIEW OF MOSAIC IMAGES

Mosaic is a type of artwork created by composing small pieces of materials, such as stone, glass, tile, etc. Invented in ancient time, they are still used in many applications today. Creation of mosaic images by computer [1] is a new research direction in recent years. Many methods have been pro- posed to create different types of mosaic images by computer. A good survey under a unified framework can be found in Battiato et al. [2] in which a taxonomy of mosaic images into four types is proposed, including crystallization mosaic, ancient mosaic, photo-mosaic, and puzzle image mosaic. The first two types are obtained from decomposing a source image into tiles (with different colors, sizes, and rotations) and reconstructing the image by properly painting the tiles, and so they both may be called tile mosaics. The other two types of mosaics are obtained by fitting images from a database to cover an assigned source image, and both may be called multi-picture mosaics. Haeberli [3] proposed a method to create crystallization mosaic images using voronoi diagrams by placing blocks at random sites and filling colors into the blocks based on the content of the original image.

Hausner [4] created ancient mosaic images by using centroidal voronoi diagrams. Dobashi et al. [5] improved the voronoi diagram to add various effects to the mosaic image, such as simulation of stained glasses. Elber and Wolberg [6] proposed a method for rendering ancient mosaics by recovering free-form feature curves from the image and laying rows of tiles along the curves. Kim and Pellacini [7] generated a kind of puzzle image mosaic, called jigsaw image mosaic, composed of many arbitrary shapes of tiles selected from a database.

Di Blasi et al. [8] presented a new puzzle image mosaic as an improvement on the jigsaw image mosaic proposed in [7] in the aspect of computation time using a suitable data structure. Di Blasi and Gallo [9] created a kind of puzzle image mosaic, which reproduces the colors of the original image and emphasizes relevant boundaries by placing tiles along the edge directions. Battiato et al. [10], [11] generated ancient mosaic images using gradient vector flows to follow the most important edges in the original image and to maximize the covered mosaic area.

Narasimhan and Satheesh [12] viewed the process of photo-mosaic generation as an optimization problem with a constraint on the repetition of a tile image and proposed a randomized iterative algorithm more efficient than the conventional genetic algorithm. By accelerating pattern searching and minimizing the memory cost, Choi et al. [13] presented a genetic feature selection method for optimization of an image set for producing photo-mosaics in real time. Battiato and Puglisi investigated 3D ancient mosaics recently.

A new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed in this study. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible. An example of such images created by the proposed method is shown in Fig. 1. Because of this characteristic of the new mosaic image, it may be used as a carrier of a secret source image in the disguise of another—a target image of a different content. This is a new technique of information hiding, not found in the literature so far. It is useful for the application of covert communication or secure keeping of secret images.

More specifically, a secret image is first divided into rectangular-shaped fragments, called tile images, which are fitted next into a target image selected from a database to create a mosaic image. The number of usable tile images for this operation is limited by the size of the secret image and that of the tile images. This is not the case in traditional mosaic image creation where available tile images for use essentially are unlimited in number because the tile images are not generated from the secret image and may be used repeatedly. Then, the information of tile-image fitting is embedded into some blocks of the mosaic image, which are selected randomly by a secret key. Accordingly, an observer possessing the key can reconstruct the secret image by retrieving the embedded information, while a hacker without the key cannot.

In this paper, a new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly losslessly from the mosaic image.

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

The proposed method is inspired by Lai and Tsai [12], in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness of Lai and Tsai [12] is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favorite image for use as the target image. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret- fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

As an illustration, Fig. 1.1 shows a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image. The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images.

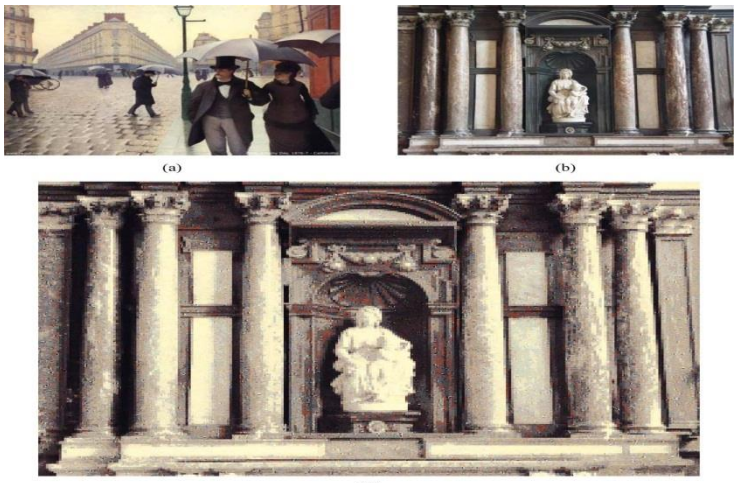

Fig. 1.1 Example of results yielded by proposed method. (a) An image. (b) Another image. (c) Secret-fragment-visible mosaic image created with (a) as secret source image and (b) as target image.

Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

In this paper the proposed method is to be applied on to a video such that a secret video is to be hidden inside the original target video.

In the remainder of this paper, the literature review is described in Section 2, the idea of the proposed method is described in Section 3. Methods to embed in video are given in section 4.

LITERATURE REVIEW

In the previous work, a secret image is first divided into rectangular-shaped fragments, called tile images, which are fitted next into a target image selected from a database to create a mosaic image. The number of usable tile images for this operation is limited by the size of the secret image and that of the tile images. This is not the case in traditional mosaic image creation where available tile images for use essentially are unlimited in number because the tile images are not generated from the secret image and may be used repeatedly. Then, the information

of tile-image fitting is embedded into some blocks of the mosaic image, which are selected randomly by a secret key. Accordingly, an observer possessing the key can reconstruct the secret image by retrieving the embedded information, while a hacker without the key cannot.

Basic Idea And Database Construction

A flow diagram of the proposed method is shown in Fig 2.1., which includes three phases of works:
Phase 1— construction of a color image database for use in selecting similar target images for given secret images;
Phase 2— creation of a secret-fragment-visible mosaic image using the tile images of a secret image and the selected similar target image as input;
Phase 3— recovery of the secret image from the created secret-fragment-visible mosaic image.

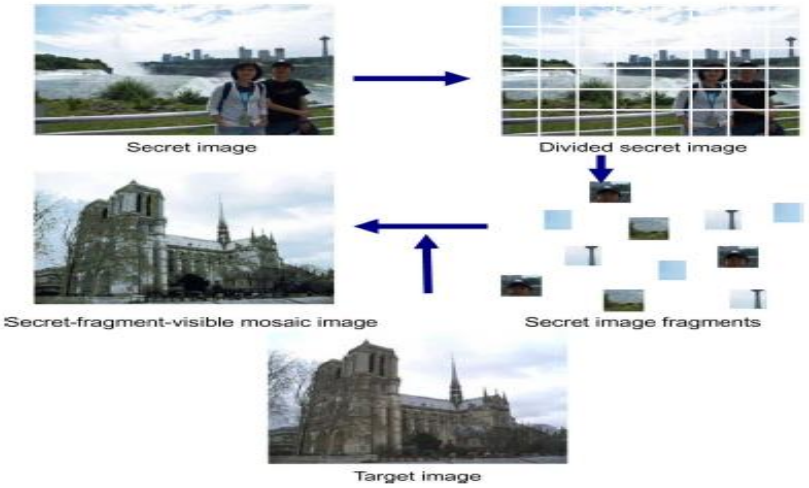

Fig. 2.1. Illustration of creation of secret-fragment-visible mosaic image.

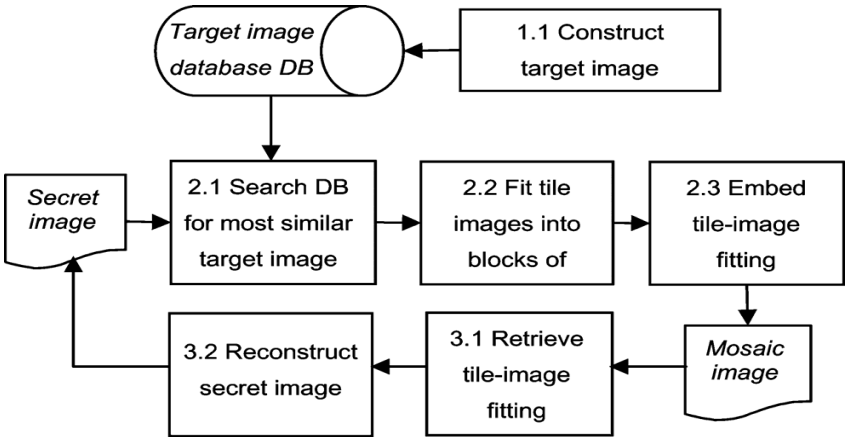

Fig. 2.2. Processes for secret-fragment-visible mosaic image creation and secret image recovery.

The first phase includes mainly the work of database construction. The second phase includes three stages of operations:

Stage 2.1—searching the database for a target image the most similar to the secret image;
Stage 2.2—fitting the tile images in the secret image into the blocks of the target image to create a mosaic image;
Stage 2.3—embedding the tile-image fitting information into the mosaic image for later secret image recovery.
And the third phase includes two stages of operations:
Stage 3.1—retrieving the previously-embedded tile-image fitting information from the mosaic image;
Stage 3.2—reconstructing the secret image from the mosaic image using the retrieved information.

But this method had many disadvantages:

- Creation of database was a hectic task and required huge amount of space which was an additional overhead
- Finding the most appropriate image from the database that would fit in was again a challenging job.
- There were also some issues found while retrieving the secret image back from the cover image.

Considering all these drawbacks into account a new method called secure image transmission technique secret-fragment-visible mosaic image by nearly reversible color transformations.

PROPOSED SYSTEM ON FRAMES

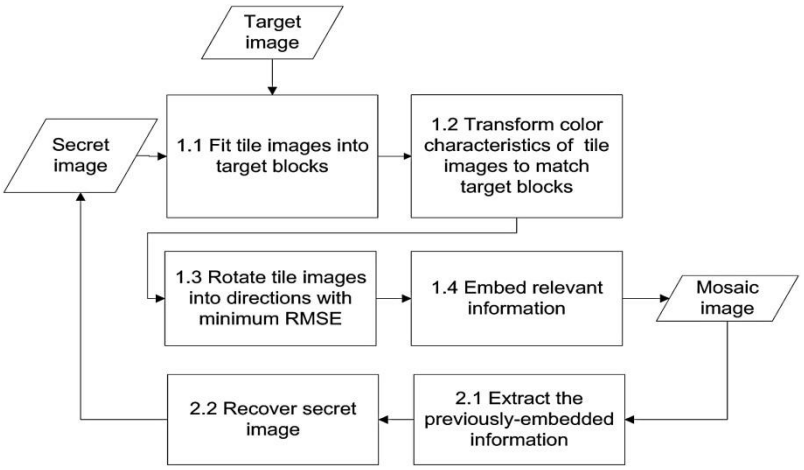

Fig. 3.1. Flow diagram of the proposed method.

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase includes four stages:

1) Fitting the tile images of the secret image into the target blocks of a preselected target image
2) Transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image;
3) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block;
4) Embedding relevant information into the created mosaic image for future Recovery of the secret image.

In the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image.

The phase includes two stages:

1) Extracting the embedded information for secret image recovery from the mosaic image, and
2) Recovering the secret image using the extracted information.

METHOD IMPLEMENTED ON VIDEOS

This system aims at securely transmitting a video by using the concept of nearly reversible color transformations on fragmented mosaic frames. This can be done using a toolbox found in MATLAB named VISION toolbox.

A GUI would display options for the user to select cover video onto which the secret video or image needs to be securely embedded. The GUI can be developed using GUIDE toolbox in MATLAB.

There would also be an option for manually selecting onto which frame of the cover video the secret video needs to be embedded .The secret video or image would be embedded by the concept described in the previous chapter ie in the form of mosaic images with nearly reversible color transformations that one can never be able to identify some secret data is embedded. The cover video as original image itself.

Moreover the embedding details, rotation details and color transformation details will be shuffled with a pseudo random number using a key value such a way that only the intended recipient who has the key will be able to retrieve back the secret data from the cover video without any distortion to both.

CONCLUSION

A new secure video transmission technique is proposed which transforms the frames of the secret video into a so-called secret fragment visible mosaic frames of the same size. The mosaic frame which looks similar to an arbitrarily selected target video frame and may be used as a camouflage of the secret frame, is yielded by dividing the secret frame into fragments and transforming their color characteristics to be those of the corresponding blocks of the target frame. Skillful techniques are designed to conduct the color transformation process and also suitable rotations of the mosaic frame is done so that the secret image may be recovered nearly losslessly and target image looks like original one. A scheme of handling the overflows/underflows in the converted pixels' color values by recording the color differences in the untransformed color space needs to be implemented.

REFERENCES

1. R. Silver and M. Hawley, Photomosaics. New York: Henry Holt,1997.
2.] S. Battiato, G. Di Blasi, G. M. Farinella, and G. Gallo, "Digital mosai framework: An overview," Eurograph.—Comput. Graph. Forum, vol.26, no. 4, pp. 794–812, Dec. 2007.
3. P. Haeberli, "Paint by numbers: Abstract image representations," in Proc. SIGGRAPH, Dallas, TX, 1990, pp. 207–214.
4. A. Hausner, "Simulating decorative mosaics," in Proc. SIGGRAPH, Los Angeles, CA, Aug. 2001, pp. 573–580.
5. Y. Dobashi, T. Haga, H. Johan, and T. Nishita, "A method for creating mosaic image using voronoi diagrams," in Proc. Eurographics, Saar- brucken, Germany, Sep. 2002, pp. 341–348.
6. G. Elber and G. Wolberg, "Rendering traditional mosaics," Vis.Comput., vol. 19, pp. 67–78, 2003.
7. J. Kim and F. Pellacini, "Jigsaw image mosaics," in Proc. SIGGRAPH, San Antonio, TX, Jul. 2002, pp. 657–664.
8. G. Di Blasi, G. Gallo, and M. Petralia, "Puzzle image mosaic," in Proc. IASTED/VIIP, Benidorm, Spain, Sep. 2005, pp. 33–37.
9. G. Di Blasi and G. Gallo, "Artificial mosaics," *Vis. Comput.*, vol. 21, pp. 373–383, 2005.
10. S. Battiato, C. Guarnera, G. Di Blasi, G. Gallo, and G. Puglisi, M.Bubak, Ed. *et al.*, "A novel artificial mosaic generation technique driven by local gradient analysis," in *Proc. ICCS*, Crakov, Poland, Jun. 2008, vol. 5102, pp. 76–85.
11. W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard*. New York, NY, USA: Van Nostrand Reinhold, 1993,pp. 34–38.
12. I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A New computer art and its application to information hiding," *IEEE Trans. Inf.Forens. Secur.*, vol. 6, no. 3, pp. 936–945, Sep. 2011.
13. E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001