A New Model of M-secure Image Via Quantization

Vijay Bhandari, Sitendra Tamrakar, Piyush Shukla and Arpana Bhandari

1 Introduction

Steganography [1–4] and steganalysis [5] have more focus in the fields concerning law enforcement [6–8] and national strategic defence. It is carving and mastery [9] of the uncover secret intelligence in the cover forum [10, 11]. Contrary between steganalysis and steganography [12, 13] is the exposure of masked secret data embedded in the cover media also called as stego image. Image encryption [9, 10] makes use of the natural possessions of an image [1, 6], such as high dismissal and well-built spatial correlation. The encryption technique protects illegal access of the data. The encrypted image [9, 14] is a noisy image such that no one can obtain the secret image [2, 9] data without the correct key. The steganography [8] contains hidden a digital picture into another cover multimedia data such as image [9] and video. Steganography technique [1–3, 6] is used when encryption [3, 4, 6] is not acceptable. The purpose of steganography [8] embeds secret data in the reselected image [9]. The structure of the paper consists of mosaic figure generation and existing work, proposed work, and the results are compared based on different parameters and conclusion.

V. Bhandari (✉)
AISECT University Bhopal, Raisen, India
e-mail: vphd2k14@gmail.com

S. Tamrakar
Christian College, Chennai, India
e-mail: drsitendra@gmail.com

P. Shukla
UIT RGPV, Bhopal, India
e-mail: pphdwss@gmail.com

A. Bhandari
CSE Department, SIRTE, Sirte, Libya
e-mail: arpanabhandari08@gmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_26

1.1 *Mosaic Figure Production and Uncover Picture Recovery Information*

1.1.1 Opting Suitable End Blocks for Every Pantile

Mosaic expression is the process of producing a picture or other florid items by combining together tiny chunks of stones and glass. The term mosaic keeps a number of tiny images called "Tiles" and is then placed on the single image called "TARGET image", before creating a mosaic image, there must be tiles embedded into the target image. The embedding of the tiles should be in the format [13, 15].

1.1.2 Mosaic Creation Using Different Similarity Measures

The source image is said to be secretly embedded in the resulting mosaic image. For creating a mosaic, the target image and the secret image can be split, but the size of splitting is different. The secret image is split for merging into a target image; the target image is split for finding the absolute place to fit the tile image in the target image [11]. In detail, the target image is split into very small tiny images and based on this, each tile image is compared with every target split image, and finds the best fit for that tile image, and in that position, the tile image is placed and so on. Generated mosaic image is the same as the target image with a little bit of quality drop. Mosaic image quality is high when splitting of the source image is high. The major difficulty is retrieving the tile images from the created mosaic images. This required the specific efficient technique for getting the secret image from the mosaic image. The creation process is done in a particular place and the retrieving process is done at another place, and for this, they can give the detail of which tile is stored in which position and the name of the image. This information is also sent to the other user so they can also be able to retrieve the image from the mosaic image [9] (Fig. 1).

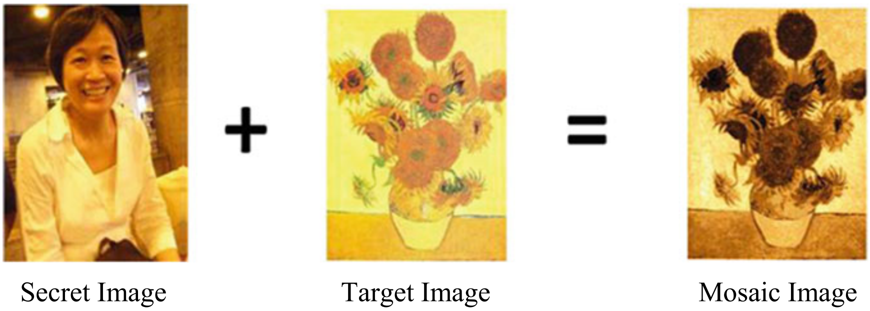

Fig. 1 Mosaic creation using different similarity measures

1.1.3 Background of Secret Image Recovery

The embedded information we have to extract to recover nearly lossless the secret image from the generated mosaic image [4].

2 Existing Work

This paper [4] introduced a colored black-and-white visual cryptography scheme, which adopts colored pixels [4] in dark descriptions to share a black and sallow top secret image. This paper [3] represents an algorithm to reversibly place a clandestine information in encrypted similes is presented, which consists of picture encryption, information embedding, and data taking out [3].

The new secret image [2] sharing scheme identifying the continuation of cheater is introduced and analyzed in this paper. A method to ensure the honesty of clandestine picture prior to its improvement is proposed.

This paper represents proposed here [6], which transforms robotically a given large-volume secret depiction into a so-called secret-fragment-visible [9, 10, 14] mosaic image of the same size [10, 14]. The mosaic image, which looks similar to an randomly elected end image and may be used as a disguise of the secret image, is yielded by dividing the clandestine image into wreckage and transforming their color uniqueness to be those of the corresponding blocks of the target image [14].

In this paper [2], the hub is on the examination of dynamic lossless data-embedding methods that allow one to embed [2] large amounts of data into digital images (or video) in such an approach that the unique image can be reconstructed [2, 10] from the watermarked picture.

3 Proposed Methodology

Mosaic image means that the image is produced by ordering many small blocks to form a vibrant larger image. The purpose of information hiding using mosaic images is a new way of securing information so that the data can be sent in a private and secure manner. The aim of this paper is to provide an efficient and better embedding algorithm as compared to all related previous techniques. The secret image is first divided into a number of blocks called “Tiles”, and then these tiles are placed on the single image called “TARGET image” which we select from our database on some similarity measures with our secret image. We are creating our own database here to overcome the drawback of managing a large database. To create a mosaic image, we have to place each and every tile of the secret image over the target image with the efficient embedding algorithm on the particular region. The embedding of the tiles should be in the format. We are using a DCT algorithm for embedding.

It involves the following steps:

First, we take a secret image which is divided into tiles, and will convert each tile image into a binary value through 16 * 16 quantization, then we prepare a form of secret value by combining all the values, and then embed this secret value in the original image through 16 * 16 quantization, after embedding, we send it to the sender who will send the data to receiver, and at the other side, the receiver will extract the secret value using the inverse algorithm which can be seen in Fig. 2.

At the first stage of transformation, we must design and partition an image into the blocks. Each block is denoted by a_i, and then 16 * 16 quantization is applied to each one of the blocks denoted by C_i.

$$C_i = T\, a_i\, T'$$

The chip rate is calculated first, which is the ratio of total no. of pixel in the host image by the no. of pixel in tile, then the value of chip rate is used to find the p_n sequence, which is an array initiated by 1 to the value of chip rate, and then temp is calculated by this chip rate and the value of temp rows and temp column is considered from all the pixel values of the cover image, the watermarked value of the pixel of the tile gets embedded in this region of temp rows and temp column.

At the second stage, quantization is the technique used in image processing to reduce the redundancies, and the lossy compression technique is used here which is achieved by compressing a range of values to an only quantum value. When the number of discrete symbols or the pixel are assigned by one constant value, and then discrete symbols which are generated as the pixels are less than this constant value

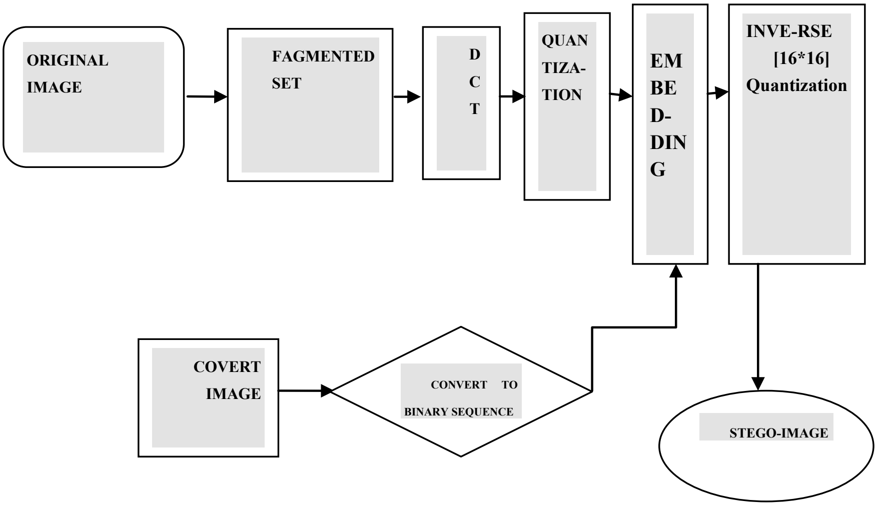

Fig. 2 Outline of the proposed work

assigned to -1 and greater than this constant value are assigned as +1, and then by this, we are able to reduce the given stream, the stream becomes more compressed.

At the third stage, the secret image should be converted into a binary sequence (m_i). This binary sequence is embedded in the middle and high-frequency region of C_i to get stego block S_i. Embedding process is based on applying magnitude modulation to the quantized value of the host 16 * 16 quantization coefficient.

$$S_i(u,v) = \begin{cases} c_i'(u, v) + \text{Qstep}\ (u, v)/3, & \text{if } m_i = 0 \\ c_i'(u, v) - \text{Qstep}\ (u, v)/3, & \text{if } m_i = 1 \end{cases}$$

m_i = each block of the secret image is converted into a binary sequence. Embedding process is based on magnitude modulation to the quantized value of the host 16 * 16 quantization coefficients. Embedding requires the selection of a suitable region in which the tile should be embedded.

At the fourth stage, for each stego block S_i (pixel value is converted in binary), the inverse 16 * 16 quantization will be applied to get the output blocks d_i, and this is the inverse process of 16 * 16 quantization as it requires to retrieve the original secret image.

$$d_i = T' S_i T$$

During extraction, the encrypted information needs to be extracted first, and then the correct sequence of tiles is obtained.

$$\begin{aligned} \text{blockSizeR} &= 100; \\ \text{blockSizeC} &= 100; \end{aligned}$$

whole BlockRows = floor(rows/blockSizeR);

Now, each of the tiles generated is then converted into binary values using

$$\text{dec2bin(message}(i, j)$$

Here, we use pseudo-random number generation for the generation of a binary key from the image. The tiny image can be used for producing RNGs and also the image from the paint software. The pixel value of the image can be generated with the simple functions in MATLAB tool and it is converted into a string value. To convert the pixel value of the image into the binary value from integer, we have to check the RGB value of the each and every pixel, and then compare the pixel value. The corresponding values (0s and 1s) are written in the text file from left to right or in any other format. If there is a small change in the image, it leads to a big difference in the generated random numbers. Here, the concatenated value of the pixel is shown:

```
1010101010110010000000000
0100011111010111000000000
1010010111110010000000000
1001011001001001000000000
0110110111111010000000000
1001011011111101000000000
0100001111111101000000000
1011111111011111000000000
0101001110101111110010100
1110101111111111111101110
1000101111111111111000010
```

From the generated binary value, embedding is performed, which embedded the secret image into the cover image and is sent to the receiver. At the receiver end, the binary value is extracted and is again converted into tile images. These tile images are then embedded to make a secret image (Fig. 3).

Here are some comparison measures, which are based on MSE, PSNR, NAE, NCC, and result analysis of the existing work and results analysis of the proposed work (Table 1).

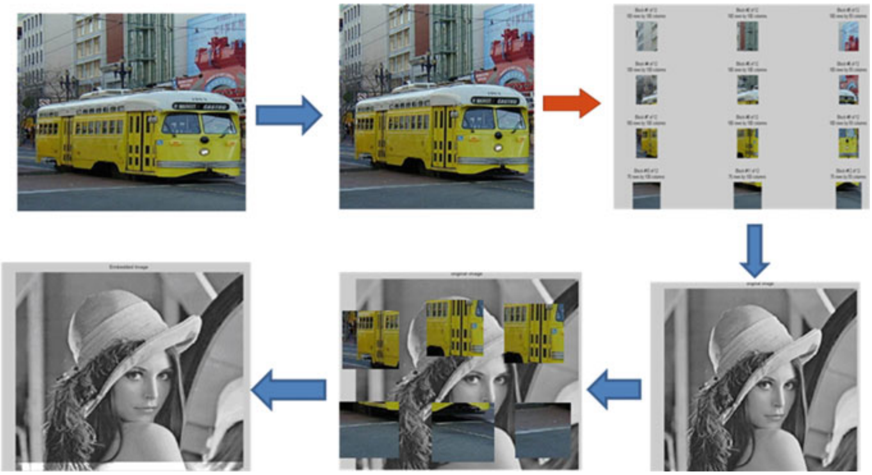

Fig. 3 Illustrations of the creation of secret-fragment-visible mosaic image

Table 1 Result analysis of the existing work and results analysis of the proposed work

No. of tiles	MSE	NAE	NCC	PSNR
6	0.22	0.0017	1.0008	54.79
12	0.21	0.0018	1.0011	54.78
15	0.31	0.0016	1.0012	55.79
18	0.29	0.0019	1.0010	54.3
20	0.30	0.0020	1.0004	55.9

3.1 Comparison Based on the Error Rate

See Fig. 4.

3.2 Comparison Based on the Computation Time

See Figs. 5 and 6.

4 Conclusion

The work that we proposed provides less compression time. This technique M-secure, here, provides a more efficient technique to authenticate the user to access the original image. By the different parameters, the work is more efficient with Ya-Lin Lee, and we have generated graphs and tables which is generated and tested through MATLAB.

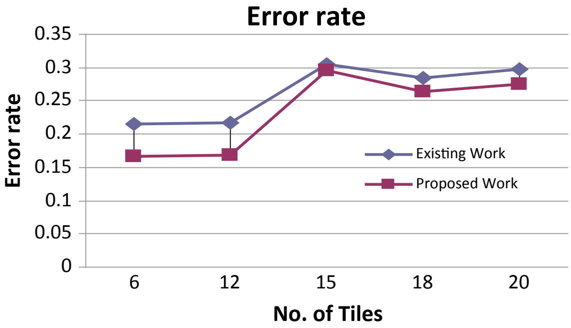

Fig. 4 Comparative analysis of error rate

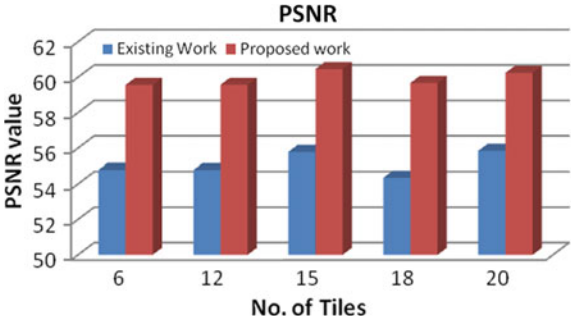

Fig. 5 Comparative analysis of computation time

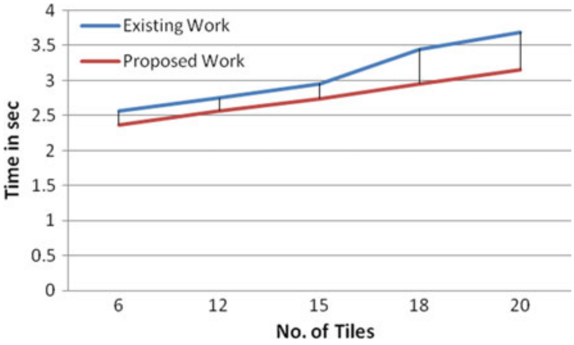

Fig. 6 Computation time in s

References

1. Ponti, M.: Image quantization as a dimensionality reduction procedure in color and texture feature extraction. Elsevier, pp. 1–12 (2015)
2. Rose, A. et al.: A secure verifiable scheme for secret image sharing. In: Second International Symposium on Computer Vision and the Internet. Elsevier, pp. 140–150 (2015)
3. Xu, D. et al.: Separable and error-free reversible data hiding in encrypted images, Elsevier, pp. 9–21 (2016)
4. Yang, C.-N. et al.: Extended color visual cryptography for black and white secret image. In: Theoretical Computer Science. Elsevier, pp. 143–161 (2016)
5. Qiao, T.: Steganalysis of jsteg algorithm using hypothesis testing theory. Springer Open J. EURASIP J. Inf. Sec. 1–16 (2015)
6. Bhandari, V., Tamrakar, S., Shukla, P.: A survey on: creation of mosaic images. In: International Conference on Advances of Electronics Computer & Mathematical Sciences (2016)
7. Chih-Wei, S., Chen, Y.-C., Hong, W.: Encrypted image-based reversible data hiding with public key cryptography from difference expansion. Published by Elsevier (2015)
8. Mishra, R. et al.: An edge based image steganography with compression and encryption. In: IEEE 2015, International Conference on Computer, Communication and Control
9. Zhou, Y. et al.: (n, k, p)-gray code for image systems. IEEE Trans. Cybern. **43**(2), 515–525 (2013)

10. Manjreka, A.: A novel approach for data transmission technique through secret fragment visible mosaic image. In: Emerging Research in Computing, Information, Communication and Applications, Springer (2015)
11. Edwina Alias, T., Mathew, D.: Steganographic technique using secure adaptive pixel pair matching for embedding multiple data types in images. IEEE, pp. 426–429 (2015)
12. Kuoa, W.-C. et al.: high capacity data hiding scheme based on multi-bit encoding function. Elsevier (2015)
13. Mishra, R. et al.: A review on steganography and cryptograph. In: 2015 International Conference on Advances in Computer Engineering and Applications. IEEE (2015)
14. Lee, Y.-L., et al.: A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. IEEE Trans. Circuits Syst. Video Technol. **24**(4), 695–704 (2014)
15. Li, X. et al.: A complete color normalization approach to histo-pathology images using color cues computed from saturation-weighted statistics. IEEE (2015)