

$International \ Journal \ of \ Innovative \ Research \ in \ Science, \ Engineering \ and \ Technology$

An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Mosaic Image Creation & Transmission Technique Based on CMYK

Ragasudha R¹, Sampathkumar K²

P.G. Student, Department of Computer Engineering, PGP College of Engineering College, Namakkal, India¹

Assistant Professor, Department of Computer Engineering, PGP College of Engineering College, Namakkal, India²

ABSTRACT: A mosaic image generation and transmission technique is proposed, which transforms automatically a given secret image into target image - called secret – fragment - visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a secret image, is yielded by dividing the secret image into fragments and transforming their colour characteristics to be those of the corresponding blocks of the target image. Skilful techniques are designed to conduct the colour transformation process so that the secret image may be recovered nearly lossless. A scheme of handling the overflows/underflows in the converted pixels' colour values by recording the colour differences in the untransformed colour space is also proposed. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. Good experimental results show the feasibility of the proposed method by using the CMYK method.

KEYWORDS: Mosaic Image, Secret Image, Target Image, CMYK Method, HSV, HLV, Secure image transmission, Data Hiding.

I. INTRODUCTION

Images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches 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. 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. Which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image. Skilful techniques are designed to conduct the colour transformation process so that the secret image may be recovered nearly lossless. 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 transforming their colour characteristics to be those of the corresponding blocks of the target image. Skilful techniques are designed to conduct the colour transformation process so that the secret image may be recovered nearly lossless. 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.

II. RELATED WORKS

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with colour corrections according to a similarity criterion based on colour variations.

The phase includes four stages:

1. Fitting the tile images of the secret image into the target blocks of a preselected target image.



International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

- 2. Transforming the colour 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 and
- 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 lossless the secret image from the generated mosaic image.

The phase includes two stages:

- I. Extracting the embedded information for secret image recovery from the mosaic image, and
- II. Recovering the secret image using the extracted information.

COLOR TRANSFORMATIONS BETWEEN BLOCKS

In the first phase of the proposed method, each tile image *T* in the given secret image is fit into a target block *B* in a preselected target image. Since the colour characteristics of *T* and *B* are different from each other, how to change their colour distributions to make them look alike is the main issue here. Reinhard *et al.* proposed a colour transfer scheme in this aspect, which converts the colour characteristic of an image to be that of another in the $l\alpha\beta$ colour space. This idea is an answer to the issue and is adopted in this paper, except that the RGB colour space instead of the $l\alpha\beta$ one is used to reduce the volume of the required information for recovery of the original secret image.

The color of each pi be denoted by (ri, gi, bi) and that of each $p_i by (r_i, g_i, b_i)$. At first, we compute the means and standard **A New Secure Image Transmission Technique** deviations of *T* and *B*, respectively, in each of the three color channels R, G, and B by the following formulas.

$$\mu_c = \frac{1}{n} \sum_{i=1}^n c_i, \quad \mu_c' = \frac{1}{n} \sum_{i=1}^n c_i'$$
$$\sigma_c = \sqrt{\frac{1}{n} \sum_{i=1}^n (c_i - \mu_c)^2}, \quad \sigma_c' = \sqrt{\frac{1}{n} \sum_{i=1}^n (c_i' - \mu_c')^2}$$

In which *ci* and *c_i* denote the C-channel values of pixels *pi* and *p_i*, respectively, ith = r, g, or *b* and C=R, G, or B. Next, we compute new colour values (*r_i*, *g_i*, *b_i*) for each *pi* in *T* by

$$c_i'' = q_c(c_i - \mu_c) + \mu_c',$$

In which $qc = \sigma_c/\sigma c$ is the standard deviation quotient and c = r, g, or b. It can be verified easily that the new colour mean and variance of the resulting tile image T_{-} are equal to those of B, respectively. In transforming the colour characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T is an issue. For this, we use the standard deviation of the colours in the block as a measure to select the most similar B for each T. Specially, we sort all the tile images to form a sequence, *Stile*, and all the target blocks to form another, *Starget*, according to the average values of the standard deviations of the three colour channels. Then, we fit the first in *Starget*, fit the second in *Starget*, and so on.



International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

III. EXPERIMENTAL RESULTS

In transforming the colour characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T is an issue. For this, we use the standard deviation of the colours in the block as a measure to select the most similar B for each T. Specially; we sort all the tile images to form a sequence, Stile, and all the target blocks to form another, Starget, according to the average values of the standard deviations of the three colour channels. Then, we fit the first in Stile into the first in Starget, fit the second in Stile into the second in Starget, and so on. Additionally, after a target block B is chosen to fit a tile image T and after the colour characteristic of T is transformed, we conduct a further improvement on the colour similarity between the resulting tile image T_{-} and the target block B by rotating T_{\perp} into one of the four directions, 00, 900, 1800, and 2700, which yields a rotated version of T with the minimum root mean square error (RMSE) value with respect to B among the four directions for final use to fit T into B. After the colour transformation process is conducted as described previously, some pixel values in the new tile image $T_{\rm might}$ have overflows or underflows. To deal with this problem, we convert such values to be nonoverflow or non underflow ones and record the value differences as residuals for use in later recovery. Specifically, we convert all the transformed pixel values in T_{-} not smaller than 255 to be 255, and all those not larger than 0 to be 0. Next, we compute the differences between the original pixel values and the converted ones as the residuals and record them as part of the information associated with T_{-} . Accordingly, the pixel values, which are just on the bound of 255 or 0, however, cannot be distinguished from those with overflow/underflow values during later recovery since all the pixel values with overflows/underflows are converted to be 255 or 0 now.



Fig. 1 Flow diagram of the Choosing Appropriate Target Blocks and Rotating Blocks

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

- a) Fitting the tile images of the secret image into the target blocks of a preselected target image.
- b) Transforming the colour characteristic of each tile image in the secret image to become that of the corresponding target block in the target image.
- c) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block.
- d) Embedding relevant information into the created mosaic image for future recovery of the secret image.



International Journal of Innovative Research in Science, Engineering and TechnologyAn ISO 3297: 2007 Certified OrganizationVolume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India



Fig. 2 Experimental result of Mosaic Image Creation.

(a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 8×8 . (d) Recovered secret image using a correct key with RMSE= 0.948 with respect to secret image (a). (e) Recovered secret image using a wrong key. (f)-(i) Mosaic images created with different tile image sizes: $16 \times 16, 24 \times 24, 32 \times 32, and 40 \times 40.$

In the second phase, the embedded information is extracted to recover nearly lossless the secret image from the generated mosaic image. The phase includes two stages:

- a) Extracting the embedded information for secret image recovery from the mosaic image and
- b) Recovering the secret image using the extracted information.

IV. FEATURE EXTRACTION

A series of experiments have been conducted to test the proposed method using many secret and target images with sizes 1024×768 or 768×1024. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (RMSE) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images. It can be seen from the figures that the created mosaic image retains more details of the target image when the tile image is smaller. It can also be seen that the block effect is observable when the image is magnified to be large; but if the image is observed as a whole, it still looks like a mosaic image with its appearance similar to the target image. A mosaic image created with smaller tile images has a smaller RMSE value with respect to the target image. On the other hand, the number of required bits embedded for recovering the secret image will be increased when the tile image becomes smaller.

In order to increase the security of the proposed method, the embedded information for later recovery is encrypted with a secret key as seen in Algorithm 1. Only the receiver who has the key can decode the secret image. However, an eavesdropper who does not have the key may still try all possible permutations of the tile images in the mosaic image to get the secret image back. Fortunately, the number of all possible permutations here is n, and so the probability for him/her to correctly guess the permutation is p=1/n! Which is very small in value? For example, for the typical case in which we divide a secret image of size 1024×768 into tile images with block size 8×8 , the value n is $(1024 \times 768)/(8 \times 8) = 12,288$. So the probability to guess the permutation correctly without the key.



International Journal of Innovative Research in Science, Engineering and Technology An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015 International Conference On Emerging Trends in Engineering and Technology (ICETET'15) On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India V. ALGORITHMS OF THE PROPOSED METHOD

Based on the above discussions, the detailed algorithms for Mosaic image creation and secret image recovery may now be described respectively as Algorithms 1 and 2.

Algorithm 1 Mosaic image creation using CMYK

Input: A secret image *S*, a target image *T*, and a secret key *K*. **Output:** A secret-fragment-visible mosaic image *F*.



Fig. 3 Correct permutations of tile images in the mosaic image without Recovering the original colour characteristics (a) correct permutation of tile Images (b) correct permutation of tile images.

Algorithm 2 Secret image recovery HSL, HSV

Input: a mosaic image F with n tile images $\{T1, T2, ..., Tn\}$ and the secret key K. **Output:** the secret image S.

VI. ACKNOWLEDGMENT

The authors would like to thank the reviewers for many useful comments and suggestions which improve the presentation of the paper.

VII. CONCLUSION

A new secure image transmission method has been proposed by using the CMYK (Cyan, Magenta, Yellow, Black), HSV (Hue Saturation Value), HSL (Hue Saturation Lightness) which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel colour transformations as well as a skilful scheme for handling overflows and underflows in the converted values of the pixels colours, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. The experimental results have shown the feasibility of the proposed method. Future studies may be directed to applying the proposed method to images of colour models other than the CMYK, HSV, and HSL.



International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

REFERENCES

[1] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption," *Opt. Commun.*, vol. 284, no. 19, pp. 4331–4339, 2011.

[2] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans.Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[3] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Colour Transfer Between Images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41,

Sep.-Oct. 2001.

[4] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," *IEEE Trans. Inf. Forens. Secur.* vol. 8, no. 5, pp. 187–193, May 2013.[21] 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.

[5] T. S. Cho, S. Avidan, and W. T. Freeman, "A probabilistic image jigsaw puzzle solver," in *Proc. IEEE CVPR*, 2010, pp. 183–190.

[6] D. Pomeranz, M. Shemesh, and O. Ben-Shahar, "A fully automated greedy square jigsaw puzzle solver," in *Proc. IEEE CVPR*, 2011, pp. 9–16.
[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284,

1998.
[8] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21,no. 3, pp. 749–761, 2004.

[9] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," *Chaos Solit. Fract.*, vol. 24, no. 3, pp. 759–765, 2005.

[10] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit..*, vol. 37, pp. 469–474, Mar. 2004.

[11] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[12] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[13] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification:Establishing equivalency between reversible data hiding and lossless data compression," *IEEE Trans. Image Process.*, vol. 22, no. 7, pp. 2775–2785, Jul. 2013.