International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 2, Issue 8, 2015, PP 23-27
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

Mosaic Images Transmission Technique for Secure Transmission

[1] B.Sai Krishna, [2] S.Sekhar Babu , [3]P.Prasanna Murali Krishna

1. (M.Tech), Department of ECE, DR.SGIT, MARKAPUR, INDIA.
2.Associate Professor, Department of ECE, DR.SGIT, MARKAPUR, INDIA.
.[3]H.O.D Department of ECE, DR.SGIT, MARKAPUR, INDIA.

Abstract: *A new secure image transmission technique is proposed, 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 into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. Skillful techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly losslessly. 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. 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.*

1. INTRODUCTION

In recent years, the topic of automatic art image creation via the use of computers arouses interests of many people and many methods have been proposed .The common goal of creating these image styles is to make the generated art images look like some other types of images. Mosaic image is also a type of computer art image is composed of many small identical tiles, such as squares, circles, triangles, and so on. Images may contain private or confidential information that should be protected from leakages during transmissions. Main two Issues in Information Hiding are: 1) Distortion rate when hiding huge amount of data 2) Selection of Matching images to the target image. So a new idea of changing an image into a cubism-like image and hiding a secret image in the cubism image using a mapping sequence is introduced that is more secure from eavesdroppers and hackers.

Currently, 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.

Picture encryption is a system that makes use of the normal property of a photo, for instance, high redundancy and strong spatial association, to get an encoded picture in light of Shannon's perplexity and dispersal properties. The encoded picture is an uproar picture so no one can obtain the puzzle picture from it unless he/she has the right key.

On the other hand, the encoded picture is a pointless record, which can't give additional information before disentangling and may energize an attacker's thought in the midst of transmission in view of its haphazardness in structure. An alternate choice for avoid this issue is data covering that covers a puzzle message into a spread picture so no one can comprehend the vicinity of the secret data, in which the data kind of the riddle message investigated in this Project a photo. Existing data disguising procedures generally utilize the systems of LSB sub circumstance, histogram moving, contrast extension, forecast blunder development, recursive histogram change, and discrete cosine/wavelet changes. On the other hand, to lessen the mutilation of the subsequent picture, an upper destined for the contortion quality is normally situated on the payload of the spread picture. An exchange on this rate mutilation issue can be found in. Along these lines, a primary issue of the systems for concealing information in pictures is the trouble to insert a lot of message information into a solitary picture. In

particular, if one needs to shroud a mystery picture into a spread picture with the same size, the mystery picture must be exceptionally packed ahead of time. For instance, for an information concealing system with an installing rate of 0.5 bits for every pixel, a mystery picture with 8 bits for each pixel must be packed at a rate of no less than 93.75% in advance so as to be covered up into a spread picture. In any case, for some applications, for example, keeping or transmitting restorative pictures, military pictures, authoritative reports, and so on., that are profitable with no stipend of genuine contortions, such information pressure operations are normally illogical.

Besides, most picture pressure systems, for example, JPEG pressure, are not suitable for line drawings and printed design, in which sharp differences between nearby pixels are frequently destructed to end up observable curios. In this Project, another system for secure picture transmission is proposed, which changes a mystery picture into an important mosaic picture with the same size and resembling a preselected target picture. The change procedure is controlled by a mystery key, and just with the key can a man recoup the mystery picture about losslessly from the mosaic picture. The proposed technique is roused by Lai and Tsai, in which another kind of PC workmanship picture, called mystery piece unmistakable mosaic picture, was proposed.

2. IMAGE ENCRYPTION

The information security is used from old ages, different person using different technique to secure their data .Following are some techniques that uses for security of images from ancient age to till date.

A. Steganography

B. Water Marking Technique

C. Visual Cryptography

D. Without sharing Keys Techniques

2.1.Steganography:

The steganography word comes from the Greek word Steganos, which is used to cover or secret and a graphy, is used for writing or drawing. Therefore, steganography is, literally, covered writing. The fundamental thought for covering the data or steganography is utilized for secure correspondence as a part of a totally imperceptible way and to abstain from attracting suspicion to the transmission of a shrouded information. Amid the transmission process, attributes of these techniques are to change in the structure and components so as not to be identifiable by human eye. Computerized features, pictures, sound records, and different documents of PC that contain perceptually critical data can be utilized as ―covers‖ or bearers to shroud mystery messages. Subsequent to inserting a message into the spread picture, an alleged ― stego image‖ is acquired.

2.2.Water Marking Technique:

Water Marking is also one of the technique used to hide the digital image, Digital watermarking is a process of embedding (hiding) marks which are typically invisible and that can be extracted only by owner‘s of the authentication. This is the technology which is used with the image that cannot be misused by any other unauthorized miss users. This technology allows anyone to do without any distortion and keeping much better quality of stegno-image, also in a secured and reliable manner guaranteeing efficient and retrievals of secret file. Digital watermarking finds wide application in security, authentication, copyright protection and all walks of internet applications. There has been effective growth in developing techniques to discourage the unauthorized duplication of applications and data. The watermarking technique is one, which is feasible and design to protect the applications and data related. The term‘ cover‘ is used to describe the original message in which it will hide our secret message, data file or image file. Invisible watermarking and visible watermarking are the two important types of the above said technology. The main objective of this package is to reduce the unauthorized duplication of applications and data, provide copyright protections, security, and authentication, to all walks of internet applications.

2.3.Visual Cryptography:

Visual Cryptography is used to hide information in images, a special encryption technique in such a way that encrypted image can be decrypted by the human eyes, if the correct key image is

used. It is uses two transparent images. One image contains image contains the secret information and the other random pixels. It is not possible to get the secret information from any one of the images. Both layers and transparent images are required to get the actual information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

2.4.Without sharing Keys Techniques:

Securing image for transmission without sharing his encrypted key, but it needs two transmission for a single image transmission, the image is encrypted with private key and is sent without sharing key to the receiver, after receiving the encrypted image receiver again encrypted the image by its own keys, and send it to the first sender, first sender removed the first encrypted key and again send to opponent, The opponent already had its keys then with this key the image is finally decrypted. Thus different person applying different-different techniques for securing his information.

3. PROPOSED METHOD

In this venture, another system for secure image transmission is proposed, which changes a secret picture into a significant mosaic picture with the same size and resembling a preselected target picture. The change procedure is controlled by a secret key, and just with the key can a man recoup the mystery picture almost losslessly from the mosaic picture. The proposed system in which another sort of PC workmanship picture, called mystery piece obvious mosaic picture, was proposed. The mosaic picture is the consequence of revision of the sections of a mystery picture in mask of another picture called the objective picture preselected from a database.

3.1.Block Diagram of the Proposed System:

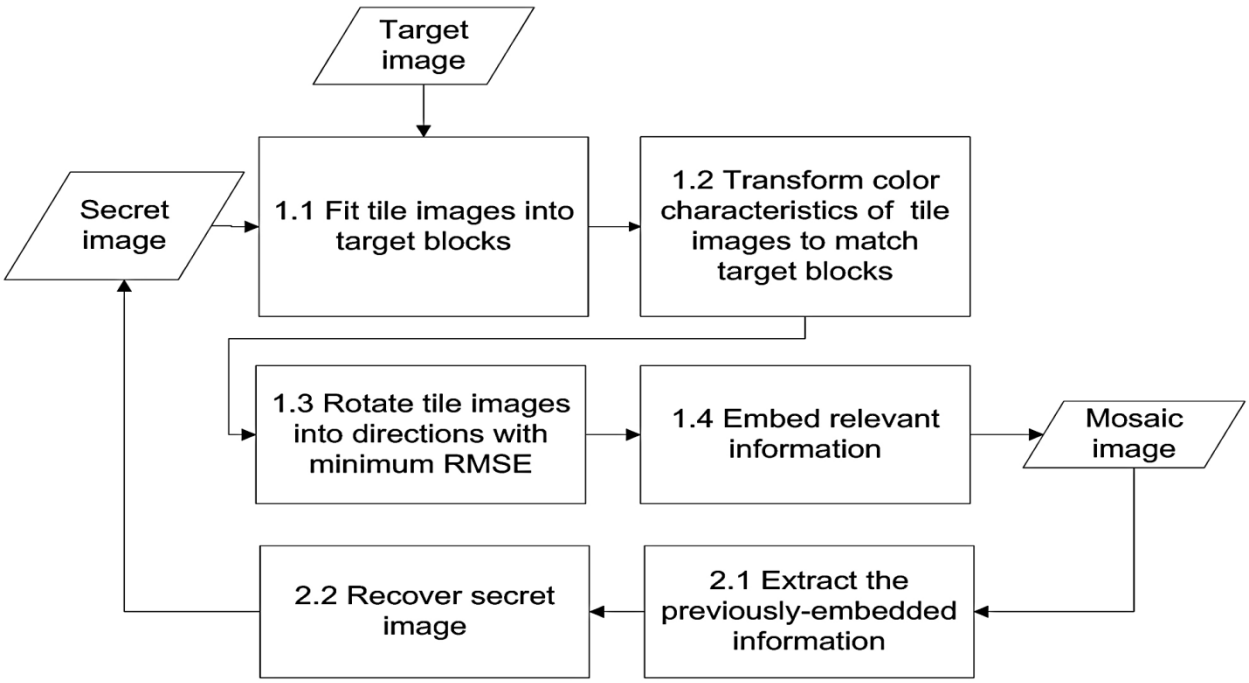

Fig 2: *Flow diagram of the proposed method.*

3.1 Skin tone detection

For color face pictures, we utilize the calculation depicted; a skin likelihood guide is made from a unique non-straight change that infuses a focused R (the red segment in RGB pictures) into its plan.

3.2 The embedding process

The focal center of this Project is to implant the mystery message in the first-level 2D Haar DWT with the symmetric-cushioning mode guided by the distinguished skin tone regions. Calculations taking into account DWT encounter some information misfortune since the converse change truncates the qualities on the off chance that they go past the lower and upper limits (i.e., 0- 255). Realizing that human skin tone dwells along the center range in the chromatic red of YCbCr shading space permits us to insert in the DWT of the Cr channel without stressing over the truncation. This would leave the

detectable quality of the stego-picture practically unaltered since the progressions made in the chrominance will be spread among the RGB hues when changed. We pick wavelets over DCT (Discrete Cosine Transform) in light of the fact that: the wavelet change imitates the Human Vision System (HVS) more nearly than DCT does; Visual curios presented by wavelets coded pictures are less clear contrasted with DCT on the grounds that the wavelets change does not decay the picture into pieces for handling. Let C and P be the spread picture and the payload individually. The stego-picture S can be acquired by the following embedding procedure.

Step 1: Encrypt P using a user supplied key to yield P'

Step 2: Generate skin tone map (*skin_map*) from the cover C and determine an agreed-upon orientation, if desired, for embedding using face features as described earlier (embedding angle will be treated as an additional secret key)

Step 3: Transform *C* to *YCbCr* colour space

Step 4: Decompose the channel *Y* by one level of 2D-DWT to yield four sub-images (*CA, CH, CV, and CD*)

Step 5: Resize *skin map* to fit *CA*

Step 6: Convert the integer part of coefficients of *CA* into the *Binary Reflected Gray Code* (*BRGC)* and store the decimal values

Step 7: Embed (the embedding location of data is also randomized using the same encryption key) the secret bits of *P'* into the *BRGC* code of skin area in *CA* guided by the *skin map*

Step 8: Convert the modified *BRGC* code back to coefficients, restore the decimal precision and reconstruct the image *Y'*

Step 9: Convert *Y'CbCr* to *RGB* colour space and obtain the stego-image, i.e., *S*. (NB: the effect of embedding is spread among the three RGB channels since the colour space was transformed).

4. CONCLUSION

A new secure image transmission method has been proposed,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 color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels' colors, secret-fragmentvisible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly losslessly from the created mosaic images. Good experimental results have shown the feasibility of the proposed method. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

REFERENCES

[1]. J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[2]. 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.

[3]. 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.

[4]. H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solit. Fract.*,vol. 32, no. 4, pp. 1518–1529, 2007.

[5]. S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps,"*Chaos Solit. Fract.*, vol. 35, no. 2, pp. 408–419, 2008.

[6]. D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption algorithm," *Chaos Solit. Fract.*, vol. 40, no. 5,pp. 2191–2199, 2009.

[7]. 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.

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

[9]. 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.

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

[11]. Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Trans.Multimedia*, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[12]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans.Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[13]. 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.

[14]. 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.

[15]. J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," *Proc. SPIE*, vol. 3971, 2001, pp. 197–208.