www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18255-18264

Optimized Secure Image Transmission approach Lossless Secret Image Recovery Based on Secret Fragmented Mosaic Images

***Ankoji Pavan** (M.Tech.)* [1] ***K. Ramanjaneyulu** M.Tech, Associate Professor* [2]

QIS College of Engineering and Technology, Ongole, Vengamukkapalem, Andhra Pradesh 523272, INDIA

chinnapavan666@gmail.com[1] ramu36nba@gmail.com[2]

Abstract

The prominence of the digital image processing is growing in the field of security, as now s days the transfer of images from one entity to another entity using internet as source of medium is increased. The digital image transmission has advanced applications in the field of security such as security related the confidentiality of medical databases, preventing leakages from the military databases, privacy protection the enterprise related documents and online document storage systems. Although lot of research has been done on secure image transmission but still it too has some unresolved issues such as leakages while transmissions and loss of the confidentiality is another drawback. An innovative approach is implemented in this paper and the main idea of the proposed work is create meaningful secret fragment mosaic image system and the important implementation in the proposed work is the secret fragment mosaic image size is same as that of preselected target image which gives scope to provide more payload capacity. The generation of the mosaic image is the resultant of the block fragments of the selected secret image and the mosaic image in the process is looks alike of the target image which is used as the source to hide the secret image by successfully transforming the color characteristics of the secret image similar to the blocks of the target image. Finally the simulation results show the performance in terms of presenting the meaningful secure image transmission technique for the lossless recovery and the necessary data is embedded into mosaic image for the recovery of the securely transmitted secret image.

Keywords: Mosaic image, Lossless recovery, Confidentiality, Secret fragment

1. INTRODUCTION

Nowadays, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Encryption of an image is a procedure which uses the natural properties of images, such as redundancy and spatial correlation, to get an image already encrypted which use the Shannon's confusion and diffusion properties. The image that is encrypted becomes an image with noise so that no one can obtain the transmitted secret image from it unless having the correct key.

Recently an innovative mechanism namely secure image transmission attracts the attention of the researchers for securely transmitting the confidentiality data through internet to the authenticated way for providing more robustness and protection against leakages while transmission. The utilization of the digital images has been increased from last few years especially in the field of the security, the frequent transmission of the digital images from one entity from the entity and the image transmission is done through the internet make human lives ease and reliable.

The transmission of the digital images through internet as medium has keep on increasing every other day because of the applications based on image transmission has been playing key role in the field of security. The main advantages of the secure image transmission are lossless

DOI: 10.18535/ijecs/v5i10.06

recovery at the recovery side and simultaneously providing better confidentiality in terms of protecting the documents related to different fields such as medicine related databases, military related datasets against leakage during transmission. The digital image transmission applications using internet as medium are illustrated in the following figure 1.1.

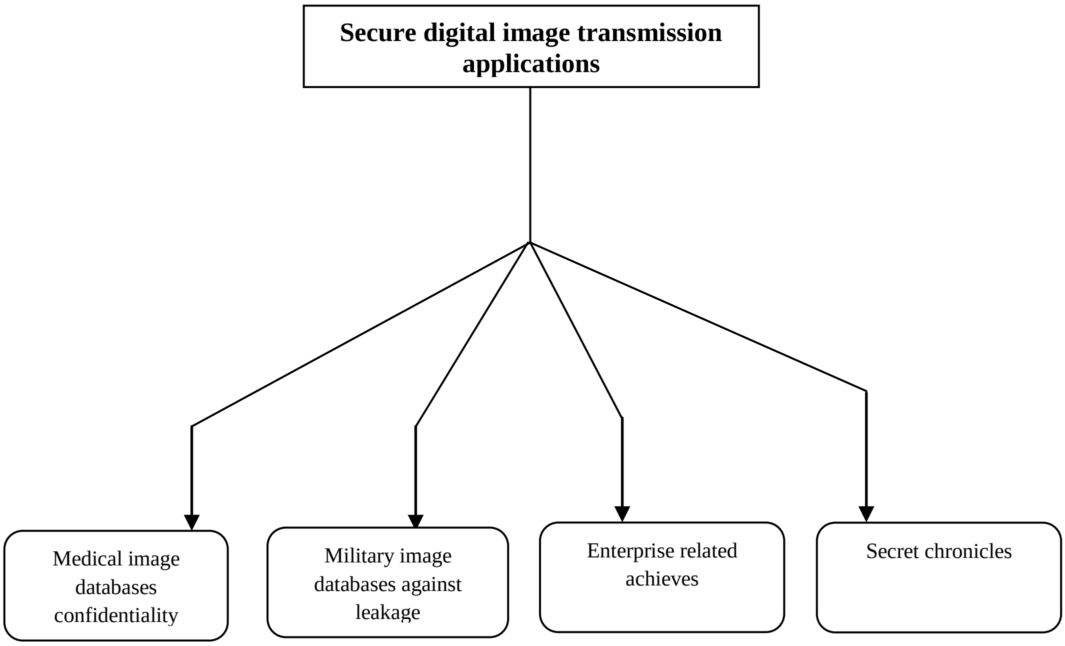
Secure digital image transmission applications
Medical image databases confidentiality
Military image databases against leakage
Enterprise related achieves
Secret chronicles

Fig.1.1: Digital image transmission applications over internet as channel

The digital images which are used for transmitting the secured data through secure image transmission application must robust against leakages and zero loss of data at the recovery end. In literature numerous works are reported on the secure image transmission and after analyzing all works the international telecom union approved two approaches namely as follows

A. Digital image encryption approach

Although tremendous progress has been made over past decades in the field of security still the transmission of data through internet and as everyday technology is changing according to that change the security norms should also change to keep confidentiality while transmission. One such approach is image encryption which uses normally the properties and characteristics of digital images to meet the practical requirement in applications related to important fields like medicine and military.

The idea behind the image encryption is to create an image with necessary secret data in it but difficult to understand the mechanism behind it. The original image characteristics are taken into consideration and convert it to the desired security norms, the reliability of the image encryption technique is no authenticated person can ever decrypt the hidden data without having the authenticated key and having the proper knowledge about the desired security norms. Digital image comprises of different properties and the image encryption approach uses the some unique properties of the image to hide the confidential data in digital content in reliable way. The digital image used in many applications should maintain the security levels in accurate way in order to provide better security to the image which is frequently utilized in the digital media in online process. The applications related to the storage and image transmission are shown in following figure.

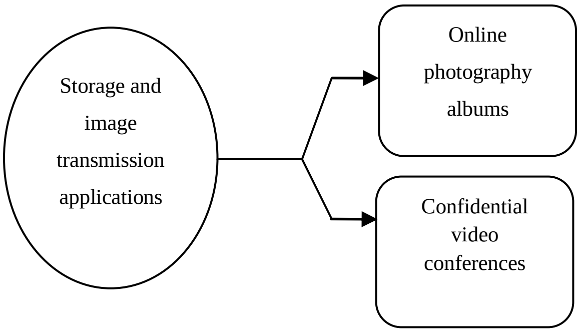
Storage and image transmission applications
Online photography albums
Confidential video conferences

Fig. 1.2: Storage and image transmission applications

In order to accomplish th task of encryption in reliable way on online storage applications lot of research has conducted in literature and after having the detailed analysis on conventional works the encryption approach are categorized into three groups as follows

(a) The encryption algorithm based on the position permutation

(b) The encryption algorithm based on valued transformation

(c) The encryption algorithm based on perceived data transformation

B. Digital image covering up approach

The image encryption has drawback of easy prediction then the covering up approach is came up with innovative idea that a mysterious element is introduced into image, in order to recover the recover the data one must first successfully crack the mysterious element place in the image which is going to transmission . The drawback facing in this approach is placing the mysterious element in the vast amount of image is concerned area.

C. Summary of the two image transmission approaches

Image encryption is an approach which commonly uses the image default approaches such as high redundancy and better correlation nature in terms spatial domain. The default properties are used for processing are depends on Shannon diffusion and as well as confusion properties. The secret encrypted image is a noisy image and the encrypted image cannot be revealed until and unless one should have authentic key. The main drawback in the image encryption approach it easily attracts the unauthenticated person attention towards it during transmission using internet as source of medium.

2. PROBLEM STATEMENT AND ITS PROMINENCE

The secure image transmission application which transmit information from one end to another plays an crucial role in technologically advanced online based digital image processing applications which mainly relates to the issue of confidentiality and lossless image recovery. The images used in online transmission mainly contain the confidential and private data related to personal and many predominant fields such as military and medicine.

The protection should be provided against unauthenticated leakages which are generally happens mainly because of the accidental/incidental attacks. A preprocessing tool is designed in this proposed work which is highly equipped algorithm to process the colorful images and create the meaningful mosaic images.

The proposed dissertation method have reliable can transform a selected secret image by secret fragment mosaic image approach where the entire transformation process is controlled by a secret key. The secret key is used later to acquired the hidden content in lossless manner from the proposed mosaic image.

3. LITERATURE SURVEY

(1) An innovative approach for hiding data the data in digital images especially mosaic images for providing robust copy right protection is presented by authors "**W. L. Lin and W. H. Tsai**" in the year 2004. The introduction of the boundary stream related to the data embedded is an idea in this approach and this boundary stream related to data are later embedded into mosaic image by detecting the respective boundary regions of preselected mosaic image in the Steganography application.

The copyright protection has been consistent concerned area in field of digital image processing and the respective method in this method helps to protect copyright protection by inserting the meaningful mosaic images into the paper copies. But this method fails when the attacks are done beyond limits.

(2) The generation of the mosaic images for protecting the copyright by using square shape tiles are introduced by S**. "C. Hung, T. Y. Liu and W. H. Tsai"** in the year 2005. The main motto of this work is creating mosaic images to embed more data but the square shape data is not always done in all applications. The mosaic image generation in other shapes can increase embedded capacity in watermarking application.

In this work the tiles used are not overlap with each others as occurs in conventional and the tiles orientation are always deterministic. The rotation and movement of tiles especially in the edges can pose problems of attacks. The work proposed in this method are tends for invisible watermarking which is used to providing robust copyright protection. This work leaves the future scope for creation of meaningful images in other shapes rather than square to increase the embedding capacity.

(3) A novel idea is proposed by "**T. C. Wang and W. H. Tsai"** in the year 2007, the proposed method mainly tends to introduce overlapping of mosaic images in horizontal and vertical tiles for the steganography application. The creation of the hole has been concerned area in the past works and that is resolved in this paper.

Although the algorithm presented in this paper has good applications in real time scenario such as communications in secret way that is technically termed as covert communication. But this work in future can improve by introducing different shapes of tiles to overlap for increasing the data hiding capacity and to create the robustness against attacks.

(4) An high equipped fast processed watermarking scheme based on Reversible contrast mapping has been implanted in the year 2007 by "**Dinu Coltuc and Jean-Marc Chassery"** to resolve two important issues which commonly faced in the past works namely resolving the high complexity issue by resulting low complexity in the results and simultaneously a new to provide robustness against all unnecessary cropping by creating the look up table.

4. PROPOSED METHOD

The proposed method mainly comprises of two important sections namely (a) generation of the mosaic images and (b) Successful recovery of the secret image. The important steps in the flow chart of the proposed method are as follows

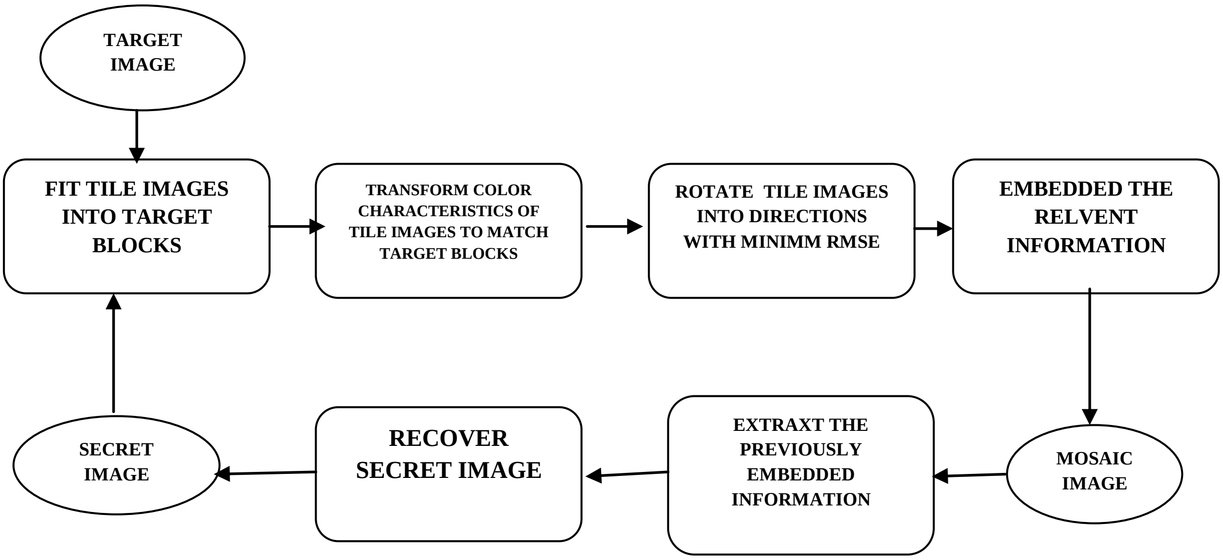
TARGET IMAGE
FIT TILE IMAGES INTO TARGET BLOCKS
TRANSFORM COLOR CHARACTERISTICS OF TILE IMAGES TO MATCH TARGET BLOCKS
ROTATE TILE IMAGES INTO DIRECTIONS WITH MINIMM RMSE
EMBEDDED THE RELVENT INFORMATION
MOSAIC IMAGE
EXTRAXT THE PREVIOUSLY EMBEDDED INFORMATION
RECOVER SECRET IMAGE
SECRET IMAGE

Figure 4.1: The secret fragment mosaic image generation flow chart

(1) In the initial phase the generation of mosaic images is done in high equipped way where the acquired mosaic images consists of the color corrected fragments of an input target image.

(2) The proposed approach has for stages as illustrated below

(a) The selection of the different tile images of the preselected secret image and fitting the selected tile images of the target images into the already generated blocks of the target image.

(b) The main challenging task in the proposed approach is transforming the every color characteristics of each tile image of secret image which corresponds to the every individual block of the respective target image.

(c) Another novel thing implemented in the proposed work is rotating each and every in the exact direction with as minimum RMSE parameter value with reference to preselected target image.

(d) the most important step is embedding the confidential information in the already generated mosaic image which is used for further recovery at the extraction in lossless recovery manner

The second phase of the secretly fragmented mosaic image includes as follows

- In the initial phase of generation of mosaic image and successful embedding of the data into mosaic image, in th second stage the extraction secret image from the already generated mosaic image in lossless manner
- Recovering the information is done by recovering the secret image which mainly uses the extracted information as reference.

A. Detailed analysis of proposed work

(1) The tile image generation is most step in the proposed work, first the images are the divided parts of the secret image, where the secret image is divided into and default shape i.e. rectangular shaped particles which is technically termed as fragments which are later used to preselected target image.

(2) Based on the color variations in the preselected target the remaining and most important process is carried on i.e. based on the resultant criteria the acquired tile images are successfully fitted into the block which are generated from the arbitrarily selected target image in reliable way.

(3) The blocks of the target image and simultaneously tile digital content of the respective secret image are color corrected so that each tile image is successfully color transformed according to those blocks of the target image.

(4) The condition inserted in the proposed work is that each and every tile image is rotated in four default directions i.e. 0^o, 90^o, 180^o or 270^o and the acquired color transformed tile images should have minimum RMSE value with reference to target image which is already preselected image.

(5) Embedding the most confidential information into mosaic image is one with reference to the RCM technique.

(6) After performing all tasks successfully an output image namely mosaic image is generated successfully with similar to the preselected target image.

B. Accurate selection of reliable target blocks for each tile image

The transformation of the color characteristics of the each tile image belongs to the secret image is performed for obtaining the better similarity in terms of color content. The color similarity is generally obtained between the each secret image tile to corresponding block of the preselected target image. But on what basis an appropriate block B is selected to tile image T is still an issue. The solution is most popular image processing parameter i.e. the standard deviation parameter is used as performance evaluator to check most B foe each respective T

A sequence is formed based on all tile images formed from the secret image S_{tile}, and simultaneously on the other end all the target blocks to form another sequence $S_{target,}$ the three colors standard deviation values form some average values and based on that average values the sequence of fitting is implemented as first in S_{tile} into the first in S_{target}, fit the second in S_{tile} into the second in S_{target} , and so on.

C. Transformations color characteristics between Blocks

In the initial approach of the proposed framework, the respective secret image tile are fit into the corresponding block of the target image and the problem arise here is make the color characteristics of two different images contents into similar one. Already many works are reported in the literature but the color transfer scheme implemented in the proposed work is realistic in nature and converts the characteristic of one in lαβ color space on behalf of other content The proposed work is also implemented on three color transform approach i.e. RGB color space instead of lαβ color space ins elected scenarios.

Let T and B be described as two pixel sets { p_1, p_2, . . . , p_n } and { p_1', p_2', . . . , p_n' }, respectively. Let the color of each p_i be denoted by (r_i, g_i, b_i) and that of each p_i' by (r_i', g_i', b_i'). At first, we compute the means and standard deviations of T and B, respectively, in each of the three color channels R, G, and B by the following formulas :

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i$$

$$\mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i{}' \qquad (1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu c)^2}$$

$$\sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i{}' - \mu c')^2} \qquad (2)$$

Where, in which c_i and c_i' denote the C-channel values of pixels p_i and p_i', respectively, with c = r, g, or b and C = R, G, or B.

Next, we compute new color values (r_i'', g_i'', b_i'') for each p_i in T by

$$c_i'' = q_c (c_i - \mu_c) + \mu_c' \qquad (3)$$

in which $q_c = \sigma_c'/\sigma_c$ is the standard deviation quotient and *c* = *r*, *g*, or *b*. It can be verified easily that the new color mean and variance of the resulting tile image T' are equal to those of B, respectively. From this, we must say that the obtained mosaic image is look similar to that of target image.

C. Rotating blocks to fit better with smaller RMSE value

After a target block B is chosen to fit a tile image T and after the color characteristic of T is transformed, we conduct a further improvement on the color similarity between the resulting tile image T' and the target block B by rotating T' into one of the four directions, 0^o, 90^o, 180^o, and 270^o, 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.

D. Embed the relevant secret image recovery information into obtained mosaic image

In order to recover the secret image from the mosaic image, we have to embed relevant recovery information into the mosaic image. For this, we adopt a technique, the reversible contrast mapping method [2] which applies simple integer transformations to pairs of pixel values. Specifically, the method conducts forward and backward integer transformations as follows, respectively, in which (*x*, *y*) are a pair of pixel values and (*x'*, *y'*) are the transformed ones

$$\begin{aligned} x' &= 2x-y \\ y' &= 2y-x \end{aligned} \qquad (4)$$

$$\begin{aligned} x &= \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil \\ y &= \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \end{aligned} \qquad (5)$$

The method yields high data embedding capacities close to the highest bit rates and has the lowest complexity reported so far.

The information required to recover a tile image T which is mapped to a target block B includes: 1) the index of B; 2) the optimal rotation angle of T; 3) the truncated means of T and B and the standard deviation quotients, of all color channels; These data items for recovering a tile image T are integrated as a four-component bit stream of the form

$$M = t_1t_2...t_mr_1r_2m_1m_2...m_{48}q_1q_2...q_{21} \qquad (6)$$

in which the bit segments represent the values of the index of *B*, the rotation angle of *T*, the means of *T* and *B*, the standard deviation quotients, respectively.

E. Total length of recovery information

The involved mean and standard deviation values are all real numbers, and it is impractical to embed real numbers, each with many digits, in the generated mosaic image. Therefore, we limit the numbers of bits used to represent relevant parameter values. Specifically, for each color channel we allow each of the means of T and B to have 8 bits with its value in the range of 0 to 255, and the standard deviation quotient q_c to have 7 bits with its value in the range of 0.1 to 12.8. That is, each mean is changed to be the closest value in the range of 0 to 255, and each q_c is changed to be the closest value in the range of 0.1 to 12.8.

In more detail, the numbers of required bits for the four data items in *M* are discussed below: 1) it needs two bits to represent the rotation angle of T because there are four possible rotation directions; 2) 48 bits are required to represent the means of T and B because we use

eight bits to represent a mean value in each color channel; 3) it needs 21 bits to represent the quotients of T over B in the three color channels with each channel requiring 7 bits. Then, the above-defined bit streams of all the tile images are concatenated in order further into a total bit stream M_t for the entire secret image, which is finally embedded into the pixel pairs in the mosaic image using the RCM technique.

So, for one tile image we required to embed 71 bit length information. and for entire secret image we requires:

Total Recovery bits have to embed = 71 bits * total no. of blocks in an image for entire secret image

Parameters	Values
Image resize to	768*1024
Divide image into blocks having block size	8*8
Each row having blocks	1024\8 = 128
Each column having blocks	768\8 = 96
Total number of blocks	128*96 = 12288
Embedding length of information for one block	71
Total length of information embedded	12288*71 = 872448

Fig. 5.5 Total length of information embedded

Algorithm 1: Mosaic image creation

Input: The input contents necessary for the creation of mosaic images are

(1) A secret image *S*,

(2) A target image T, and

(3) A secret key K.

Output: The collaboration of all three input contents with necessary processing steps results in generation of a secret-fragment-visible mosaic image F.

Stage 1: Fitting the tile images into the target blocks

Step 1: Change the sizes of target image T and secret image S and make them identical. (here we resize both to 768*1024); and divide the secret image into *n* tile images as well as the target image into *n* target blocks with each being of equal size. (Here each block/tile of 8*8 size)

Step 2: Compute the means and the standard deviations of each tile image and each target block for the three color channels, and compute accordingly the average standard deviations for each individual of them.

Step 3: According to values of average standard deviation obtained, keeping it in ascending order, sort the tile images and the target blocks in separate sets.; map in order the blocks in the sorted tile set to those in the sorted target set in a 1-to-1 manner; and reorder the mappings according to the indices of the target images, new sequence named as L.

Step 4: The final step in the accurate fitting tile in the necessary block target image are done according to the new sequence generated

Stage 2: Performing color conversions between the tile images and the target blocks

Step 5: Create a counting table TB with 256 entries, each with an index corresponding to a residual value (where, each residual value will be in the range of 0 to 255), and assign an initial value of zero to each entry.

Step 6: For each mapping, represent the means of tile image and target block, present at that particular mapping point, respectively, by eight bits; and represent the standard deviation quotient *qc* by seven bits, where *c* = *r*, *g*, or *b*.

Step 7: For each pixel p_i in each tile image T_i of mosaic image F with color value c_i where c = r, g, or b, transform c_i into a new value $c_i^{''}$ by (3); if $c_i^{''}$ is not smaller than 255 or if it is not larger than 0, then change $c_i^{''}$ to be 255 or 0, respectively.

Stage 3: Rotating the tile images

Step 8: Compute the RMSE values of each color transformed tile image T_i in F with respect to its corresponding target block B_{ji} after rotating T_i into each of the directions $\theta = 0^o$, 90^o, 180^o and 270^o; and fix the rotation of T_i into the optimal direction θ^o with the smallest RMSE value.

Stage 4: Embedding the secret image recovery information.

Step 9: For each tile image T_i in mosaic image F, construct a bit stream M_i for recovering T_i, in the way as described in section 4.4, including the bit-segments which encode the data items of: 1) the index of the corresponding target block B_{ji}; 2) the optimal rotation angle θ° of T_i; 3) the means of T_i and B_{ji} and the related standard deviation quotients of all three color channels.

Step 10: Concatenate the bit streams M_i of all T_i in F in a raster-scan order to form a total bit stream M_t; use the secret key K to encrypt M_t into another bit stream $M_t^{'}$; and embed $M_t^{'}$ into F by the reversible contrast mapping scheme.

Step 11: Obtain the final form of a secret-fragment-visible mosaic image F.

5. RESULTS AND ANALYSIS

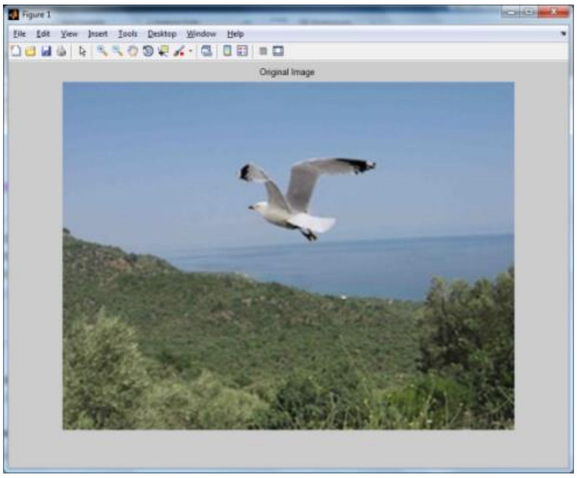

Figure 5.1: Original image

Analysis

The original is also termed as target image which plays crucial role in generating secure mosaic fragmented image to provide robust secure image transmission approach

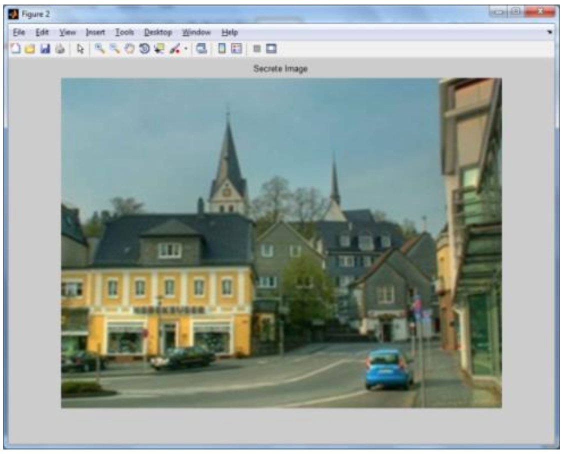

Figure 5.2: Secret image

Analysis

The selection of the different tile images of the preselected secret image and fitting the selected tile images of the target images into the already generated blocks of the target image.

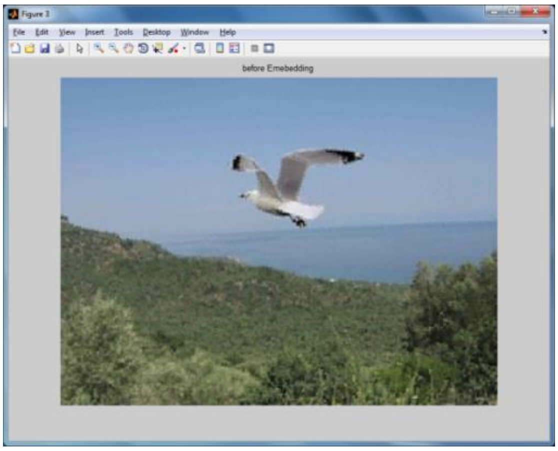

Figure 5.3: Before embedding mosaic image

Analysis

The before embedding mosaic image is an image where the confidential data is not embedded it is the step where the fitting of block and tile happened.

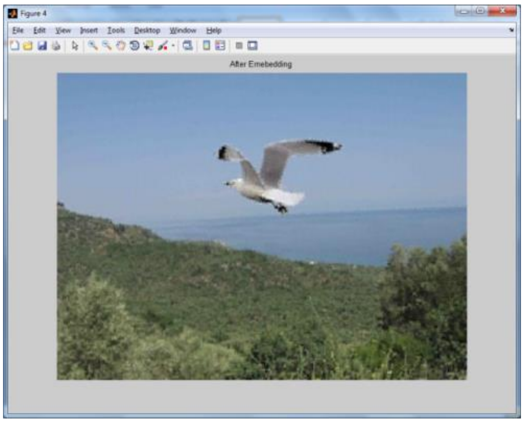

Figure 5.4: After embedding mosaic image

Analysis

The after embedding mosaic image is an image where the confidential data is embedded it is the step where the fitting of block and tile has completed

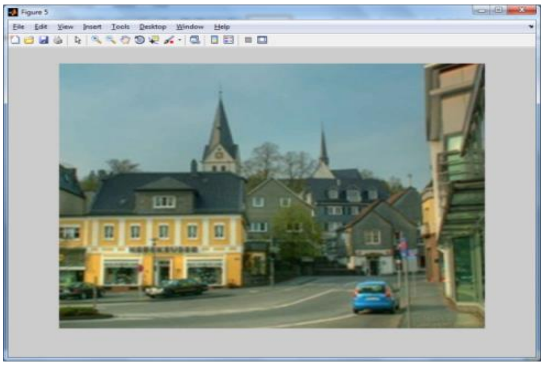

Figure 5.5: Extracted image

Analysis

The extraction of the data is done in lossless manner by successfully from the secret fragmented mosaic image

6. CONCLUSION

The secure image transmission is used to improve the security norms while transmitting the data related confidential filed using internet as source of medium. The proposed secret fragment image algorithm has recorded good advantages over the conventional approaches to protect the privacy information while transmission. Although enormous research have been made in the past years over data hiding in digital content but still secure image transmission is still concerned as concerned area in the field of digital image processing, as reported in the literature the drawbacks such as low embedding capacity, scope for incidental/ accidental attacks etc. In our proposed method a analytical approach is presented where instead of one secret image one can embed multiple secret images in digital video and the experimental results shows the good performance and better efficiency.

EXTENSION

The proposed method has been written on the digital images, in this work images are used as media to hide the secret image by using the an approach where mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. So in extension work we did the same algorithm on the digital videos. The approach towards videos are totally different from the images, so algorithm on videos is the contribution to the proposed work.

REFERENCES

[1] 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.

DOI: 10.18535/ijecs/v5i10.06

[2] D. Coltuc and J.-M. Chassery, “Very fast watermarking by reversible contrast mapping,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.

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

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] D. Xiao, X. Liao, and P. Wei, “Analysis and improvement of a chaos based image encryption algorithm,” Chaos Solit. Fract., vol. 40, no. 5, pp. 2191–2199, 2009.