NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 4, Apr.-2017

IMPLEMENTATION OF ROBUST AND ACCURATE SECURE DATA TRANSMISSION BASED ON SECRET-FRAGMENT-VISIBLE MOSAIC IMAGE

PRIYANKA ZANWAR
E&Tc, KSIET, HINGOLI, Priyankazanwar1@gmail.com

PROF. G. UBALE
E&Tc, KSIET,HINGOLI

ABSTRACT:

The internet security has become the important criteria in the 21st century security applications and its prominence is increasing along with the implementation of the innovative technologies. The data transmission based algorithms has gained popularity in the security domain to provide the protection to the secret information in a reliable way. The secure data transmission is been a concerned area in the field of security and the accidental/incidental attacks on secure data makes it more challenging to provide the ample security without any flaws. The secure image transmission technique paid a lot of attention from the research organizations because of its unique ability to recover the secret image almost losslessly. Although tremendous progress has been made in the past decade on this area but it is consider as unresolved issue in the security domain of the digital image processing domain. The novelty of the proposed method is it automatically transforms the large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. In order to convert the secret image into a mosaic image make use of color transformations is done by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. A scheme namely lossless hiding scheme is utilized along with the key which is used to recover the secret image from the mosaic image by using the information which is embedded into mosaic image. The reliability and efficiency of the proposed method are evaluated by simulation results.

KEYWORDS: Internet security, Data transmission, Mosaic image, Color transformations, Color characteristics.

1. INTRODUCTION:

The inventions and technological innovations have not only changed the word but also make the 21st century as "era of the technology" and the security domain has become the integral part of the each application to provide the ample security to the information. The security domain reaches to next level with the introduction of the digitalization and the applicative algorithms such as Cryptography, Steganography and Watermarking have changed facet of modern security standards. The digitalization collaboration with the internet has introduced the revolutionary changes in the security standards and the secure data transmission has been a research area from years which needs depth research to make it hacking free and attacks free.

The digital image usage has increased tremendously in the modern world and its presence can be visualized in the renowned research fields such as robotics, medicine, genetics, satellite image processing, security, computer vision and so on. The transmission of the digital images through internet has increased due to various reasons and the flaws associated with it also increased in unimaginable manner. The secure data transmission intention is to provide the security to private information and to the confidential data. To provide the security to the confidential data through transmission is a challenging task as it suffers from the frequent leakages possesses high level security risks to the secured data. The diagrammatic representation of the online data transmission is as follows

Fig. 1: The figure of online data transmission

In 21stcentury digital image play the crucial role to meet the human daily requirements in reliable and efficient way. The digital image processing domain is categorized into various areas namely the area of

security, the area of biometrics, the area of satellite image processing, the area of medical image processing and the practical image processing applications like compression, enhancement, restoration etc. In current scenario the digital images plays prominent role in daily lives and as well as high equipped professional needs. Nowadays transmission of digital images through internet has been increasing day by day through social networking sites, online personal albums, cloud storage and as well as high equipped professional areas confidential enterprise archives and high end areas like medical imaging systems, and military image databases.

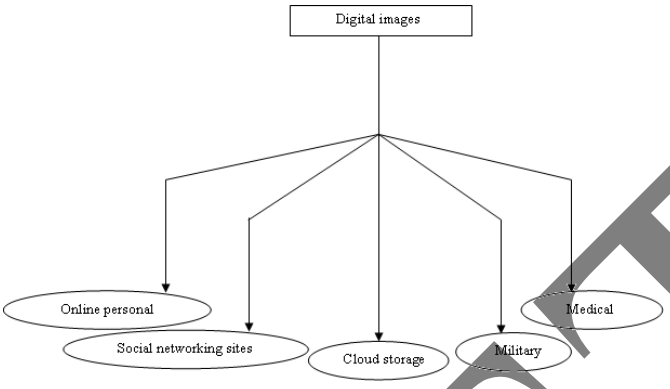

Fig. 2: Digital images and its usage application areas

The respective digital which are widely used in various applications are usually contain private or confidential information relates to military or any private organization. The research work in the literature shows the importance of the secure image transmission and the works reported in the literature presents the advantages and disadvantages of the secure image transmission. The most important drawback facing in the image transmission is leakages during transmissions.

In this study, a new approach is proposed for the secure image transmission which is focused to transform a secret image into the respective meaningful mosaic image. The transformed mosaic image is of same size as target image and it must look like the preselected target image. The secret key is generated in this approach which control the transformation process in well defined manner and the same key is used by the user to recover the secret image nearly losslessly from the mosaic one. The proposed approach is considered as the computer art image and called as secret-fragment-visible mosaic image, was proposed.

2. RELATED CONTENT:

(I) IMAGE ENCRYPTION:

The development achieved in the past years in security field made it more robust against the attacks, but still the data transmission through internet is challenging the standards of the security algorithms and the robust algorithms which achieved the accurate results in data hiding fails to maintain their reliability in the transmission. The image encryption privacy and it provides the ample security measures to the data. The security in the encryption algorithm depends on the "KEY" and it stops the unauthenticated user to read the confidential information without approval. The image encryption algorithm utilizes the unique properties of the image to provide the robustness. The data storage and image transmission are diagrammatically shown as follows

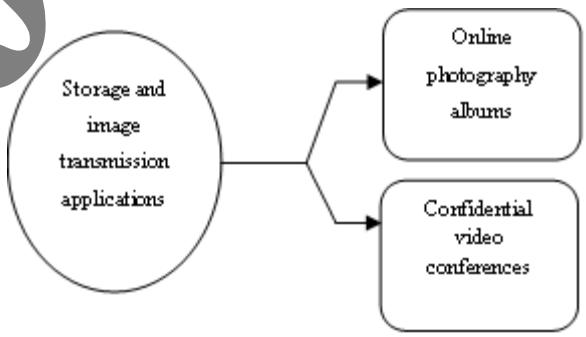

Fig. 1.3: Storage and image transmission applications

The image encryption algorithms are categorized into three segments as follows

- The position permutation based algorithms are considered as initial encryption works reported in the literature

- The valued transformation based encryption algorithms are followed by the position permutation which are widely used in the high profile applications
- The data transformation in terms of color or any other content is the third segment of the image encryption and the condition of the data transformation is the operation must be perceptible to the human visual system

(II) COVERING UP APPROACH:

The prediction of the hidden secret image is a drawback in the image encryption and the solution to this problem is covering up the secret image with any other content which perfectly hides the secret image behind it with robust behavior. The mysterious aspect which hides encrypts along with secret image is transmitted with it till it reach the destination in hassle free manner. The mysterious aspect conquers the large space which might be a limitation when transferring the large amount of data.

3. PROBLEM DEFINITION:

The digitally transmitted information has become the integral part of the various applications which has a vital role in many daily needs in terms of confidential privacy. The advancement in the technology introduces high level risk factors and fails to provide the ample security measurements. The information related to the prominent fields such as medicine and military are highly sensitive and needs to provide high level security cover when it is transmitted through the online as the attackers easily grab the information in a fraction of time.

The proposed achieves the reliability in the secure image transmission along with robustness against the attacks and the key generation is the important aspect which prevents the grabbing of confidential information in online transmission. The algorithm has ability to handle the transmission even in the worst situations.

4. PROPOSED METHODOLOGY:

The proposed study is composed of two prominent segments as follows

- The mosaic image generation is performed at the initial phase
- The secret image recovery is the second implementation followed by the mosaic image generation

The generation of the mosaic images is considered as the crucial aspect in the proposed study and the mosaic image which is generated is composed of color corrected fragments as of input image. The preselected secret image and the target image have huge importance in the proposed study, where tile images of the preselected image are selected and the selected tile images are well fitted in the target image blocks. The transformation of color characteristics for each selected tile image corresponding to the target image block. The rotation of the tile image in exact desired direction with minimum RMSE value with reference to preselected target image. The confidential information is embedded into the generated mosaic image is recovered in a lossless manner at the extraction process.

- The secretly fragmented image includes the following

The successful embedding of the confidential information in the mosaic image and its lossless extraction is the initial work carried out in this segment. The extraction of the secret image utilizes the reliability of proposed work to achieve the accuracy.

(I) DETAILED ANALYSIS:

(1) The first step in the proposed method is to divide the secret image into tile images with a specific size as well as divide the target image into block image. Segmentation of images is technically called as fragments, which are used to hide the tile images with respect to block image.

(2) Compute the mean and standard deviation of the tile image and block image with respect to three different color channels. Based on the average standard deviation value the mosaic image is generated.

(3) The next step is to sort the tile image and block image according to the average standard deviation value and sort the tile image block into target image block in an 1-by-1 manner with respect to their positions.

(4) Standard deviation coefficients (**QC**) are generated by the ratio of standard deviation of target image to the secret image. $\mathbf{q_c}$ consists of 7 bits ranges from 0.1 to 12.8.

(5) Compute the RMSE value of the tile image with respect to the block image after every rotation of tile image at an angle 0^o, 90^o, 180^o, and 270^o and note down the residual value. Rotation of an image can be done only at smaller RMSE value.

(6) To retrive the secret image from the mosaic image a bit stream is generated with respect to standard deviation coefficient, target blocks, tile image and the indices.

(7) The secret key is generated to avoid the secret image get hacked as well as to provide a better security to the secret image.

(II) THE TARGET BLOCKS SELECTION FOR EACH TILE IMAGE IN ACCURATE MANNER:

To obtain the best similarity of color content, the transformation of the color characteristics is performed on tile image that belongs to the secret image.

The similarity of the color will be obtained between the each secret image tile to the corresponding block of the preselected target image. But there an issue, i.e. for tile image T on what basis appropriate block b is selected. There is a solution for this issue named as the standard deviation parameter. It is most popular image processing parameter. By using this parameter performance can be evaluated to check most B for each respective T.

From the secret image S_{tile} a sequence is formed based on all tile images. Equally from the target blocks another sequence is formed i.e. S_{target} ,from some average values the three color standard deviation values are taken based on that values sequence 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.

(III) TRANSFORMATIONS COLOR CHARACTERISTICS BETWEEN BLOCKS:

In the initial approach of the projected framework, the various secret image tile square measure match into the corresponding block of the target image and therefore the downside arise here is create the colour characteristics of 2 totally different pictures contents into similar one. Already several works square measure reported within the literature however the colour transfer theme enforced within the projected work is realistic in nature and converts the characteristic of 1 in lαβ color house on behalf of different content The projected work is additionally enforced on 3 color rework approach i.e. RGB color house rather than lαβ color house ins elective eventualities.

Let Tand Bbe 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 Tand B, respectively, in each of the three color channels R, G, and B by the following formulas :

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

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

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

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

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 band C = R, G, or B.

Next, we compute new color values (r_i'', g_i'', b_i'') for each $p_i$in Tby

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

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 andvariance 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.

(IV) ROTATING BLOCKS TO FIT BETTER WITH SMALLER RMSE VALUE:

After a target block B is chosen to suit a tile image T and when the colour characteristic of T is remodeled, we have a tendency to conduct an extra improvement on the colour similarity between the ensuing tile image T' and therefore the target block B by rotating T' into one in every of the four directions, 0^o, 90^o, 180^o, and 270^o, that yields a turned version of T' with the minimum root mean sq. error (RMSE) worth with relation to B among the four directions for final use to suit T into B.

(V) EMBED THE RELEVANT SECRET IMAGE RECOVERY INFORMATION INTO OBTAINED MOSAIC IMAGE:

In order to recover the key image from the mosaic image, we've to implant relevant recovery data into the mosaic image. For this, we tend to adopt a method, the reversible distinction mapping technique [2] that applies easy number transformations to pairs of pel values. Specifically, the tactic conducts forward and backward number transformations as follows, severally, during which (x, y) area unit a combine of pel values and (x', y') area unit the reworked ones

$$x' = 2x - y \qquad (4)$$

$$y' = 2y - x$$

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

$$y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil$$

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 Twhich is mapped to a target block Bincludes: 1) the index of B; 2) the optimal rotation angle of T; 3) the truncated means of T and Band the standard deviation

quotients, of all color channels; These data items for recovering a tile image Tare integrated as a four-component bit stream of the form

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

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.

(VI) 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 Tand 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 Tand Bbecause we use eight bits to represent a mean value in each color channel; 3) it needs 21 bits to represent the quotients of Tover Bin 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:

5. RESULTS AND ANALYSIS:

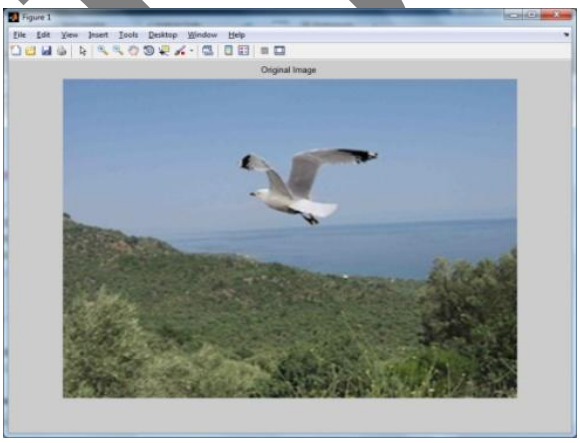

Figure 5.1: Original image

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

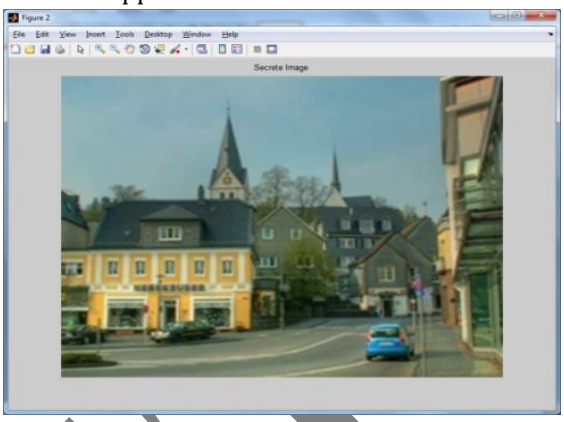

Figure 5.2: Secret image

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.

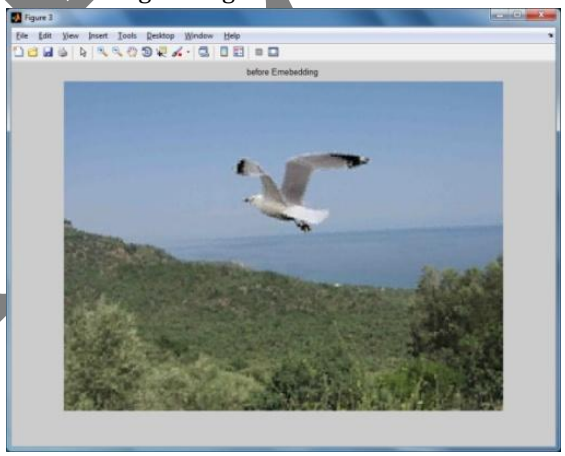

Figure 5.3: Before embedding mosaic image

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.

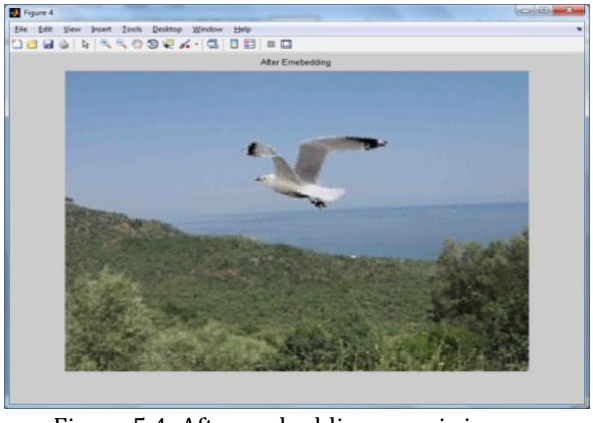

Figure 5.4: After embedding mosaic image

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

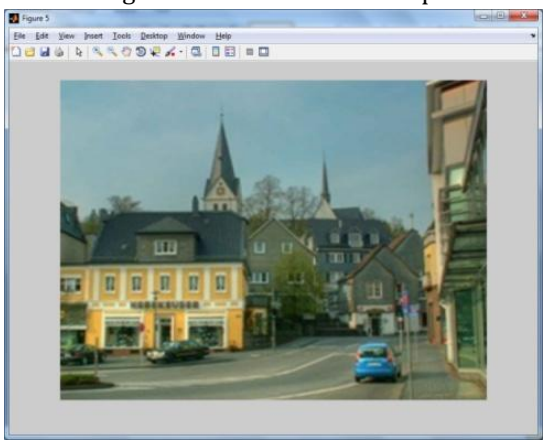

Figure 5.5: Extracted image

ANALYSIS:

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

6. CONCLUSION:

The mosaic image transmission is one of the scheme used to transform a meaningful secret image into a mosaic image with high security as well as reliability against the conventional methods. Pixel color transformation is used to handle the overflows and underflows of pixels at the encryption process to provide the highest visual quality. Here the secret image is segmented into tile images which is also called as fragments. Mosaic Image is created with respect to the fragments of the target image to provide high security. A secret key is also embedded to improve the security of the secret image. Also the original secret image is decrypted from the mosaic image with any loss of data.As a result the simulation analysis shows better efficiency with high security. Ain the future work video is used to hide the secret image.

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.
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.