ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Fast Image Encryption and Decryption Scheme via Secret - Fragment -Visible Mosaic Images

Konduru Mani
PG Scholar,
Department of ECE,
MJR College of Engineering & Technology,
Piler, A.P - 517214, India.

D.Dhana Sekhar
Assistant Professor,
Department of ECE,
MJR College of Engineering & Technology,
Piler, A.P - 517214, India.

ABSTRACT

Another protected picture transmission strategy is proposed, which changes consequently a given huge volume mystery picture into a supposed mystery part unmistakable mosaic picture of a similar size. The mosaic picture, which seems to be like a self-assertively chose target picture and might be utilized as a cover of the mystery picture, is yielded by isolating the mystery picture into sections and changing their shading attributes to be those of the relating squares of the objective picture. Adroit strategies are intended to lead the shading change process with the goal that the mystery picture might be recuperated almost lossless. A plan of taking care of the floods/sub-currents in the changed over pixels' shading esteems by recording the shading contrasts in the untransformed shading space is additionally proposed. The data required for recouping the mystery picture is implanted into the made mosaic picture by a lossless information concealing plan utilizing a key. As in eradication a similar paper will be exchange the picture through the video and additionally the flag commotion proportion of the mystery – part obvious mosaic picture likewise decreased. Great trial comes about demonstrate the practicality of the proposed.

File Terms: ***Color change, information concealing, picture encryption, mosaic picture, and secure picture transmission.***

1. INTRODUCTION

Right now, pictures from different sources are much of the time used and transmitted through the web for different applications, for example, online individual photo collections, private undertaking files, archive stockpiling frameworks, restorative imaging frameworks, and military picture databases. These pictures as a rule contain private or secret data with the goal that they ought to be shielded from spillages amid transmissions [1]. As of late, numerous strategies have been proposed for securing picture transmission, for which two normal methodologies are picture encryption and information stowing away. Picture encryption is a method that makes utilization of the common property of a picture, for example, high repetition and solid spatial relationship, to get an encoded picture in view of Shannon's perplexity and dissemination properties. The encoded picture is a commotion picture with the goal that nobody can acquire the mystery picture from it unless he/she has the right key. In any case, the scrambled picture is a futile record, which can't give extra data previously unscrambling and may stir an assailant's consideration amid transmission because of its haphazardness in shape. An other option to maintain a strategic distance from this issue is information concealing that shrouds a mystery message into a cover picture so nobody can understand the presence of the mystery information, in which the information sort of the mystery message examined in this paper is a picture. Existing information concealing strategies principally use the systems of LSB sub circumstance [2-5], histogram moving, distinction extension, expectation

Cite this article as: Konduru Mani & Dhana Sekhar, "A Fast Image Encryption and Decryption Scheme via Secret -Fragment -Visible Mosaic Images", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 3, 2018, Page 29-41.

blunder development, recursive histogram alteration, and discrete cosine/wavelet changes. Be that as it may, keeping in mind the end goal to diminish the twisting of the subsequent picture, an upper destined for the mutilation esteem is typically determined to the payload of the cover picture. An exchange on this rate twisting issue can be found in . Along these lines, a principle issue of the strategies for concealing information in pictures is the trouble to insert a lot of message information into a solitary picture. In particular, on the off chance that one needs to shroud a mystery picture into a cover picture with a similar size, the mystery picture must be exceptionally compacted ahead of time. For instance, for an information concealing strategy with an inserting rate of 0.5 bits for every pixel, a mystery picture with 8 bits for every pixel must be packed at a rate of no less than 93.75% already keeping in mind the end goal to be covered up into a cover picture. In any case, for some applications, for example, keeping or transmitting restorative pictures, military pictures, authoritative reports, and so forth., that are important with no recompense of genuine twists, such information pressure operations are typically unfeasible. Also, most picture pressure techniques, for example, JPEG pressure, are not appropriate for line illustrations and printed designs, in which sharp complexities between nearby pixels are regularly destructed to end up noticeably discernible relics. In this paper, another method for secure picture transmission is proposed, which changes a mystery picture into a significant mosaic picture with a similar 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 almost losslessly [6]from the mosaic picture. The proposed strategy is propelled by Lai and Tsai, in which another kind of PC workmanship picture, called mystery piece obvious mosaic picture, was proposed. The mosaic picture is the aftereffect of modification of the pieces of a mystery picture in camouflage of another picture called the objective picture preselected from a database. In any case, an undeniable shortcoming of Lai and Tsai is the necessity of a vast picture database so that the created mosaic picture can be adequately like the chose target picture. Utilizing their strategy, the client isn't permitted to choose uninhibitedly his/her most loved picture for use as the objective picture [7]. It is accordingly wanted in this investigation to evacuate this shortcoming of the technique while keeping its legitimacy, that is, it is expected to outline another strategy that can change a mystery picture into a mystery part unmistakable mosaic picture of a similar size that has the visual appearance of any unreservedly chose target picture without the need of a database.

Fig. 1. Result yielded by the proposed technique. (a) Secret picture. (b) Target picture. (c) Secret-section obvious mosaic picture made from (an) and (b) by the proposed strategy.

As a representation, Fig. 1 demonstrates an outcome yielded by the proposed strategy. In particular, after an objective picture is chosen discretionarily, the given mystery picture is first separated into rectangular pieces called tile pictures, which at that point are fit into comparative squares in the objective picture, called target hinders, as per a comparability basis in view of shading varieties. Next, the shading normal for each tile picture is changed to be that of the comparing target hinder in the objective picture, bringing about a mosaic picture which resembles the objective picture. Significant plans are likewise proposed to direct about lossless recuperation of the first mystery picture from the subsequent mosaic picture. The proposed strategy is new in that a significant mosaic picture is made, interestingly with the picture encryption technique that lone makes good for nothing clamor pictures. Likewise, the proposed technique [8-10] can change a mystery picture into a masking mosaic picture without pressure, while an information concealing strategy must shroud an exceptionally compacted form of the mystery picture into a cover picture when the mystery picture and the cover picture have similar information volume.

II. CONVENTIONAL METHODS

In the image-processing applications, the conventional methods that are most frequently used are cryptography, watermarking and steganography using Least-Significant Bit (LSB) Algorithm [3-7]. Cryptography [9] is the method in which encryption and decryption are performed based on the secret key, which is known only to the sender and receiver. The original information is embedded by following some encoding process in which the data is re-inserted based on certain procedure. In order to decode the message at the receiver, the reverse process is followed which is done at the encoding process. The difference between steganography and cryptography is that

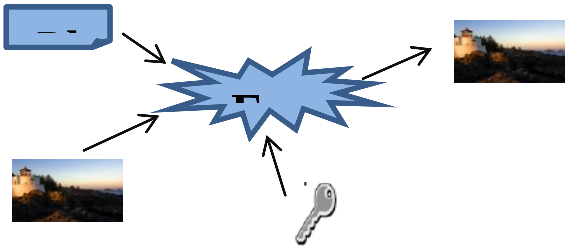


Fig.2 (a). Encryption Process

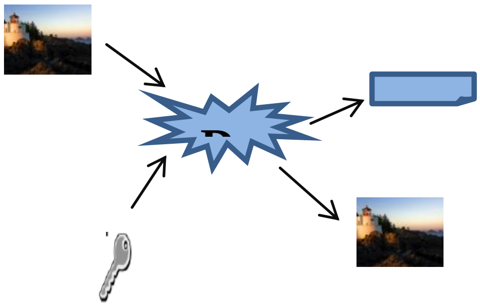


Fig.2 (b). Decryption Process

Cryptography is preferred to keep the contents of the message secretly whereas steganography is the method which keeps the existence of the message secret. These two methods protect information from the unwanted parties and security attacks. The other technology that is closely related to these methods is digital water-marking, in which an image is embedded into the original image such that it helps in signifying the ownership for the purpose of copyright protection[5]. Water-marking technique enables the intellectual property of the owner to identify the customers who break their licensing agreement by supplying the property to third parties. Fig.2(a) and 2(b) represents the encryption and decryption processes in cryptography [11]. This paper describes the steganography algorithm that is most suitable for business and in commercial applications.

III. 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

A) STEGANOGRAPHY

The steganography word comes from the Greek word Steganos, which is used to covered or secret and a graphy is used for writing or drawing. Therefore, steganography is, literally, covered writing. The main idea for covering the information or steganography is used for secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4]. During the transmission process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital videos, images, sound files, and other files of computer that contain perceptually important information can be used as –covers‖ or carriers to hide secret messages. After embedding a message into the cover-image, a so-called –stego image‖ is obtained.

In [2] Security, Capacity and robustness are three different aspects which is affecting steganography and its usefulness. Capacity is used to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper‘s inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information. The concept of the mosaic images in [1] was created perfectly and it has been widely used. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in

[2]. In the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics.

B) 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 in [15] 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 [12]. 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.

C) 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. The technique was propose by Naor and Shamir in 1994[1]. 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 or 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.

D) WITHOUT SHARING KEYS TECHNIQUES

The author at [11] is securing image for transmission without sharing his encrypted key, but it needs two transmission for a single image transmission, In [11]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 it‘s keys then with this key the image is finally decrypted. Thus different person applying different-different techniques for securing his information.

IV. IDEAS OF THE PROPOSED METHOD

The proposed method includes two main phases as shown by the flow diagram of Fig. 2 : 1) mosaic image creation and 2) secret image recovery In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) transforming the color 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 [13] 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 losslessly the secret image from the generated mosaic image. The phase includes two stages: 1) extracting the embedded information for secret image recovery from the mosaic image, and 2) recovering the secret image using the extracted information.

A) COLOUR TRANSFORMATIONS BETWEEN BLOCKS

In the primary period of the proposed strategy, each tile picture T in the given mystery picture is fit into an objective square B in a preselected target picture. Since the shading qualities of T and B are not quite the same as each other, how to change their shading dispersions to influence them to resemble the other alike is the fundamental issue here. Reinhard et al. proposed a shading move conspire in this perspective, which changes over the shading normal for a picture to be that of another in the lαβ shading space. This thought is a response to the issue and is received in this paper, aside from that the RGB shading space rather than the lαβ one is utilized to lessen the volume of the required data for recuperation of the first mystery image.More particularly, let T and B be portrayed as two pixel sets {p1, p2, . . . , pn} and {p_1, p_2, . . . , p_ n }, separately.

Give the shade of every pi a chance to be signified by (ri, gi, bi) and that of each p_ I by (r_ I, g_ I, b_ I). At in the first place, we register the methods and standard deviations of T and B, separately, in each of the three shading channels R, G, and B by the accompanying equations:

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

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

in which ci and c_i denote the C-channel values of pixels pi and p_ i, respectively, 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 pi in T by

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

in which qc = σ _ c/σc 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. To compute the original color values (ri, gi, bi) of pi from the new ones (r__ i , g__ i , b__ i), we use the following formula which is the inverse of (3):

$$c_i = (1/q_c)(c_i'' - \mu_c') + \mu_c.$$

Furthermore, we have to embed into the created mosaic image sufficient information about the new tile image T_ for use in the later stage of recovering the original secret image. For this, theoretically we can use (4) to compute the original pixel value of pi. However, the involved mean and standard deviation values in the formula 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 in (3) and (4). 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 qc in (3) 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 qc is changed to be the closest value in the range of 0.1 to 12.8. We do not allow qc to be 0 because otherwise the original pixel value cannot be recovered back by (4) for the reason that 1/qc in (4) is not defined when qc =0.

B) CHOOSING APPROPRIATE TARGET BLOCKS AND ROTATING BLOCKS TO FIT BETTER WITH SMALLER RMSE VALUE

In transforming the color 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 colors 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 color channels [14]. 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 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, 0o, 90o, 180o, and 270o, which yields a rotated version of T_ with the minimum root mean square error (RMSE) [15] value with respect to B among the four directions for final use to fit T into B.

C) HANDLING OVERFLOWS/UNDERFLOWS IN COLOR TRANSFORMATION

After the color transformation process is conducted as described previously, some pixel values in the new tile image T_ might have overflows or underflows. To deal with this problem, we convert such values to be non-overflow or non-under flow 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. To remedy this, we define the residuals of those pixel values which are on the bound to be 0 and record them as well. However, as can be seen from (3), the ranges of possible residual values are unknown, and this causes a problem of deciding how many bits should be used to record a residual. To solve this problem, we record the residual values in the untransformed color space rather than in the transformed one. That is, by using the following two formulas, we compute first the smallest possible color value cS (with c = r, g, or b) in T that becomes larger than 255, as well as the largest possible value cL in T that becomes smaller than 0, respectively, after the color transformation process has been conducted

$$c_S = \lceil 1(/q_c)(255 - \mu_c') + \mu_c \rceil \,;$$
$$c_L = \lfloor (1/q_c)(0 - \mu_c') + \mu_c \rfloor \,.$$

Next, for an untransformed value ci which yields an overflow after the color transformation, we compute its residual as |ci - cS|; and for ci which yields an underflow, we compute its residual as |cL - ci|. Then, the possible values of the residuals of ci will all lie in the range of 0 to 255 as can be verified. Consequently, we can simply record each of them with 8-bits. And finally, because the residual values are centralized around zero, we use further in this study the Huffman encoding scheme to encode the residuals in order to reduce the number of required bits to represent them.

D) EMBEDDING INFORMATION FOR SECRET IMAGE RECOVERY

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 proposed by Coltuc and Chassery [4] and apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Unlike the classical LSB replacement methods [8], [15], [16], which substitute LSBs with message bits directly, the reversible contrast mapping method [14] 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

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

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 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; and 4) the overflow/underflow residuals. These data items for recovering a tile image T are integrated as a five-component bit stream of the form M = t1t2. . .tmr1r2m1m2. . .m48q1q2. . .q21d1d2. . .dk in which the bit segments t1t2 . . . tm, r1r2, m1m2 . . . m48, q1q2. . . q21, and d1d2 . . . dk represent the values of the index of B, the rotation angle of T, the means of T and B, the standard deviation quotients, and the residuals, respectively. In more detail, the numbers of required bits for the five data items in M are discussed below: 1) the index of B needs m bits to represent, with m computed by

$$m = \lceil \log[(W_S \times H_S)/N_T] \rceil$$

in which WS and HS are individually the width and tallness of the mystery picture S, and NT is the extent of the objective picture T; 2) it needs two bits to speak to the pivot point of T on the grounds that there are four conceivable turn bearings; 3) 48 bits are required to speak to the methods for T and B since we utilize eight bits to speak to a mean an incentive in each shading channel; 4) it needs 21 bits to speak to the remainders of T over B in the three shading channels with each channel requiring 7 bits; and 5) the aggregate number k of required bits for speaking to every one of the residuals relies upon the quantity of floods or undercurrents in T_. At that point, the above-characterized bit surges of all the tile pictures are connected all together further into an aggregate piece stream Mt for the whole mystery picture. Additionally, keeping in mind the end goal to shield Mt from being assaulted, we scramble it with a mystery key to get an encoded bit stream M_ t , which is at long last installed into the pixel combines in the mosaic picture utilizing the technique for Coltuc and Chassery [4] depicted previously. It might require more than one cycle in the encoding procedure since the length of M_ t might be bigger than the quantity of pixel sets accessible in an emphasis. A plot of the insights of the quantities of required bits for mystery picture recuperation is appeared in Fig. 8(b). Also, we need to insert too some related data about the mosaic picture age process into the mosaic picture for use in the mystery picture recuperation process. Such data, depicted as a bit stream I like M specified beforehand, incorporates the accompanying information things: 1) the quantity of emphases led in the process for inserting the bit stream M_t ; 2) the aggregate number of utilized pixel matches in the last emphasis for installing M_ t ; and 3) the Huffman table for encoding the residuals. With the bit stream M_ t implanted into the mosaic picture, we can recoup the mystery picture back as will be depicted later. It is noticed that some misfortune will be caused in the recouped mystery picture, or all the more particularly, in the shading change process utilizing (3), where every pixel's shading esteem ci is duplicated by the standard deviation remainder qc, and the subsequent genuine esteem c__ I is truncated to be a number in the scope of 0 through 255. Be that as it may, in light of the fact that each truncated part is littler than the estimation of 1, the recuperated estimation of ci utilizing (4) is as yet sufficiently exact to yield a shading almost indistinguishable to its unique one. Notwithstanding when floods/undercurrents happen at a few pixels in the shading change process, we record their lingering esteems as portrayed beforehand and subsequent to utilizing (4) to recoup the pixel esteem ci, we add the remaining esteems back to the figured pixel esteems ci to get the first pixel information, yielding an almost losslessly recuperated mystery picture. As per the consequences of the trials led in this paper, each recuperated mystery picture has a little RMSE esteem as for the first mystery picture.

V. SECURE IMAGE TRANSMISSIONS

The information into the original information. The word Steganography is derived from the Greek words "stegos" meaning "cover" and "graphic" which means "writing". In most of the image processing applications, Steganography is used to hide the information in the images.

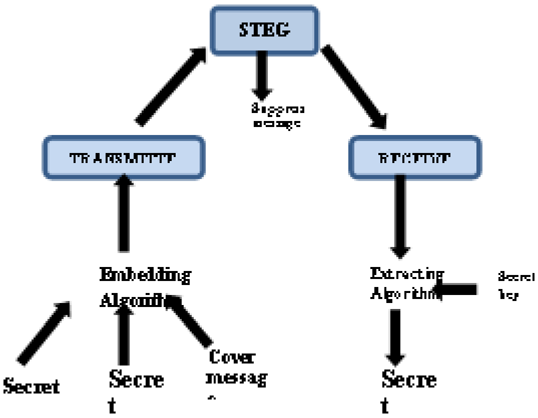


Fig.3. Basic Steganography System Scenario

Information security is the protection of the image and the systems or hardware that is used to store and transmit the images. Stegnography is the most efficient method through which the existence of the message can be kept secret. This can be accomplished through hiding the information in another image, video or audio file [1][2]. .Hence the existing information is hidden secretly. Stegangraphy supports different types of digital formats that are used for hiding the data. These files are known as carrier files. To achieve a high performance approach, both embedding ratio and image quality are considered as important issues. This paper presents the high-performance on achieving security. The steganography system scenario is shown in figure.1

VI. PROPOSED METHOD

SKIN TONE DETECTION:

For colour face images, we use the algorithm described in [1], a skin probability map is created from a special non-linear transformation that injects a zeroed R (the red component in RGB images) into its formulation.

THE EMBEDDING PROCESS

The central focus of this paper is to embed the secret message in the first-level 2D Haar DWT with the symmetric-padding mode guided by the detected skin tone areas.

Algorithms based on DWT experience some data loss since the reverse transform truncates the values if they go beyond the lower and upper boundaries (i.e., 0- 255). Knowing that human skin tone resides along the middle range in the chromatic red of *YCbCr* colour space allows us to embed in the DWT of the *Cr* channel without worrying about the truncation. This would leave the perceptibility of the stego-image virtually unchanged since the changes made in the chrominance will be spread among the *RGB* colours when transformed. We choose wavelets over DCT (Discrete Cosine Transform) because: the wavelet transform mimics the Human Vision System (HVS) more closely than DCT does; Visual artefacts introduced by wavelets coded images are less evident compared to DCT because the wavelets transform does not decompose the image into blocks for processing. Let *C* and *P* be the cover-image and the payload respectively. The stego-image *S* can be obtained by the following embedding procedure:

STEP 1: Encrypt P using a user supplied key to yield

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,CD)

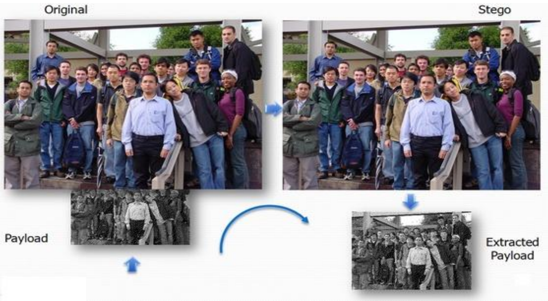
STEP 5: Resize skin_map to fit CA

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

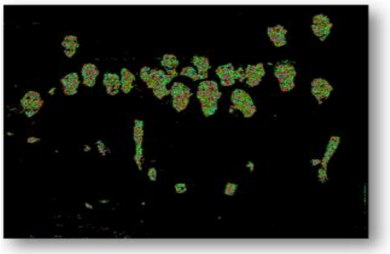
STEP 7: Embed (the embedding location of data is also randomized using the same encryption key) the secret bits of P' into the BRGC code of skin area in CA guided by the skin_map

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).



(A)



(B)

Fig. 4(A,B). Hiding data in human skin tone areas, bottom shows the differences between the original and stego-images.

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

Input: a secret image *S*, a target image *T*, and a secret key *K*.

Output: a secret-fragment-visible mosaic image *F*.

Stage 1. Fitting the tile images into the target blocks.

Step 1. If the size of the target image *T* is different from that of the secret image *S*, change the size of *T* to be identical to that of *S*; and divide the secret image *S* into *n* tile images *{T*1, *T*2, . . . , *Tn}* as well as the target image *T* into *n* target blocks *{B*1, *B*2, . . . , *Bn}* with each *Ti* or *Bi* being of size *NT* .

Step 2. Compute the means and the standard deviations of each tile image *Ti* and each target block *Bj* for the three color channels according to (1) and (2); and compute accordingly the average standard deviations for *Ti* and *Bj* , respectively, for *i* = 1 through *n* and *j* = 1 through *n*.

Step 3. Sort the tile images in the set *Stile* = *{T*1, *T*2, . . . , *Tn}* and the target blocks in the set *Starget* = *{B*1, *B*2, . . . , *Bn}* according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted *Stile* to those in the sorted *Starget* in a 1-to-1 manner; and reorder the mappings according to the indices of the tile images, resulting in a *mapping sequence L* of the form: *T*1 → *Bj*1 , *T*2 → *Bj*2 , . . . , *Tn* → *Bjn* .

Step 4. Create a mosaic image *F* by fitting the tile images into the corresponding target blocks according to *L*.

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, and assign an initial value of zero to each entry (note that each residual value will be in the range of 0 to 255).

Step 6. For each mapping *Ti* →*Bji* in sequence *L*, represent the means μc and μ _ c of *Ti* and *Bji*, respectively, by eight bits; and represent the standard deviation quotient *qc* appearing in (3) by seven bits, according to the scheme described in Section III(A) where *c* = *r*, *g*, or *b*.

Step 7. For each pixel *pi* in each tile image *Ti* of mosaic image *F* with color value *ci* where *c* = *r*, *g*, or *b*, transform *ci* 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; compute a residual value *Ri* for pixel *pi* by the way described in Section III(C); and increment by 1 the count in the entry in the counting table *TB* whose index is identical to *Ri*.

Stage 3. rotating the tile images.

Step 8. Compute the RMSE values of each color transformed tile image *Ti* in *F* with respect to its corresponding target block *Bji* after rotating *Ti* into each of the directions θ =0o, 90o, 180o and 270o; and rotate *Ti* into the *optimal* direction θo with the smallest RMSE value.

Stage 4. embedding the secret image recovery information.

Step 9. Construct a Huffman table *HT* using the content of the counting table *TB* to encode all the residual values computed previously.

Step 10. For each tile image *Ti* in mosaic image *F*, construct a bit stream *Mi* for recovering *Ti* in the way as described in Section III(D), including the bit-segments which encode the data items of: 1) the index of the corresponding target block *Bji*; 2) the optimal rotation angle θ° of *Ti*; 3) the means of *Ti* and *Bji* and the related standard deviation quotients of all three color channels; and 4) the bit sequence for overflows/underflows with residuals in *Ti* encoded by the Huffman table *HT* constructed in Step 9.

Step 11. Concatenate the bit streams *Mi* of all *Ti* in *F* in a raster-scan order to form a total bit stream *Mt* ; use the secret key *K* to encrypt *Mt* into another bit stream *M_ t* ; and embed *M_ t* into *F* by the reversible contrast mapping scheme proposed in [24].

Step 12. Construct a bit stream *I* including: 1) the number of conducted iterations *Ni* for embedding *M_ t*; 2) the number of pixel pairs *Npair* used in the last iteration; and 3) the Huffman table *HT* constructed for the residuals; and embed the bit stream *I* into mosaic image *F* by the same scheme used in Step 11.

ALGORITHM 2 SECRET IMAGE RECOVERY

Input: a mosaic image *F* with *n* tile images *{T*1, *T*2, . . . ,*Tn}* and the secret key *K*.

Output: the secret image *S*.

Stage 1. extracting the secret image recovery information.

Step 1. Extract from *F* the bit stream *I* by a reverse version of the scheme proposed in [24] and decode them to obtain the following data items: 1) the number of iterations *Ni* for embedding *M_ t* ; 2) the total number of used pixel pairs *Npair* in the last iteration; and 3) the Huffman table *HT* for encoding the values of the residuals of the overflows or underflows.

Step 2. Extract the bit stream *M_ t* using the values of *Ni* and *Npair* by the same scheme used in the last step.

Step 3. Decrypt the bit stream *M_ t* into *Mt* by *K*.

Step 4. Decompose *Mt* into *n* bit streams *M*1 through *Mn* for the *n to-be-constructed* tile images *T*1 through *Tn* in *S*, respectively.

Step 5. Decode *Mi* for each tile image *Ti* to obtain the following data items: 1) the index *ji* of the block *Bji* in *F* corresponding to *Ti*; 2) the optimal rotation angle *θ*° of *Ti*; 3) the means of *Ti* and *Bji* and the related standard deviation quotients of all color channels; and 4) the overflow/underflow residual values in *Ti* decoded by the Huffman table *HT*.

Stage 2. recovering the secret image.

Step 6. Recover one by one in a raster-scan order the tile images *Ti*, *i* = 1 through *n*, of the desired secret image *S* by the following steps: 1) rotate in the reverse direction the block indexed by *ji*, namely *Bji*, in *F* through the optimal angle *θ*° and fit the resulting block content into *Ti* to form an *initial* tile image *Ti*; 2) use the extracted means and related standard deviation quotients to recover the original pixel values in *Ti* according to (4); 3) use the extracted means, standard deviation quotients, and (5) to compute the two parameters *cS* and *cL*; 4) scan *Ti* to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there; 5) add respectively the values *cS* or *cL* to the corresponding residual values of the found pixels; and 6) take the results as the final pixel values, resulting in a *final* tile image *Ti*.

Step 7. Compose all the final tile images to form the desired secret image *S* as output.

VII.Experimental Results

A progression of investigations have been led to test the proposed strategy utilizing numerous mystery and target pictures with sizes 256 ×256. To demonstrate that the made mosaic picture resembles the preselected target picture, the quality metric of root mean square blunder (RMSE) is used, which is characterized as the square foundation of the mean square distinction between the pixel estimations of the two pictures. A case of the trial comes about is appeared; Fig. 5(a)&5(b) demonstrates the made mosaic picture utilizing Fig. 3 as the mystery picture and Fig. 4 as the objective picture of size 8x8 and 16x16. The tile picture measure is 8×8. The recuperated mystery picture utilizing a right key is appeared in Fig. 6 which looks almost indistinguishable to the first mystery picture appeared in Fig. 3 as for the mystery picture. It is noted by the way that the various test comes about appeared in this paper have target versus mosaic, as observed in Fig.8. Additionally, Fig. 7 demonstrates the recuperated mystery picture utilizing a wrong key, which is a clamor picture. Fig. 6(a), 6(b) indicate more outcomes utilizing diverse tile picture sizes. It can be seen from the assumes that the made mosaic picture holds more points of interest of the objective picture when the tile picture is littler. It can likewise be seen that the blockiness impact is detectable when the picture is amplified to be substantial; however in the event that the picture is seen all in all, despite everything it resembles a mosaic picture with its appearance like the objective picture. Fig. 8 demonstrates the diagram between target picture Vs mystery pictures. Fig 9 (a) RMSE for mystery picture Vs separated picture Fig 9 (b) required bits for mystery picture Vs extricated picture.

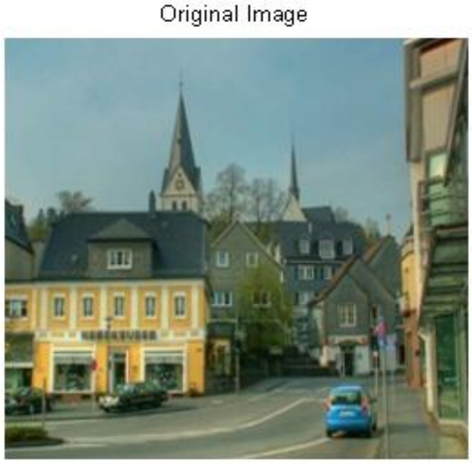


Fig.5. original image

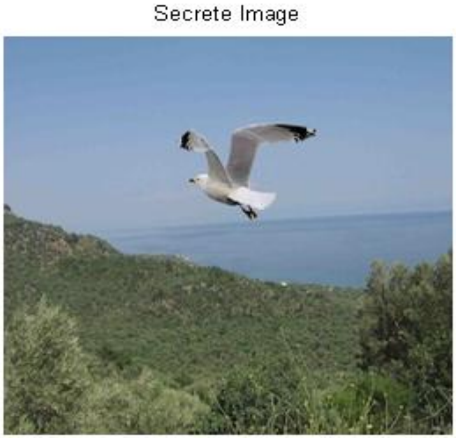


Fig.6. secret image

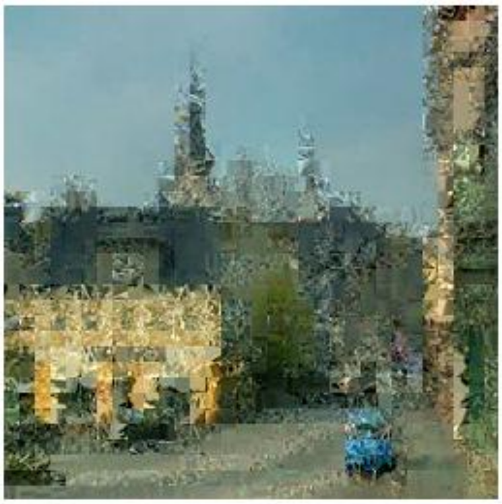


Fig.7(a). Mosaic image created by using 8×8

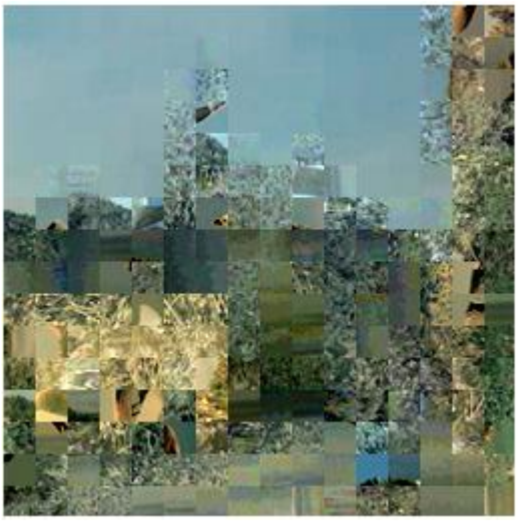


Fig. 7(b). Mosaic image created by using 16× 16

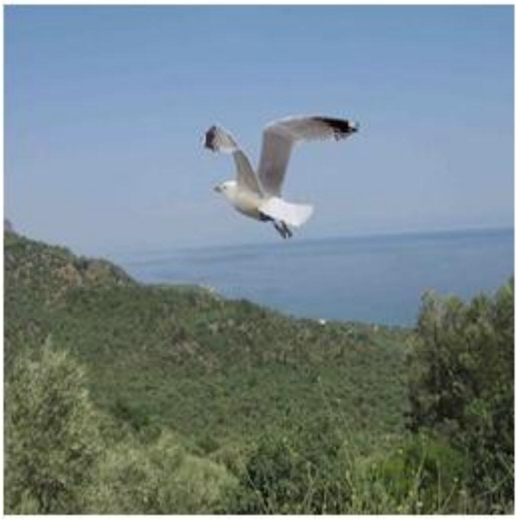


Fig.8(a). Extracted Secrete Image by using 8×8

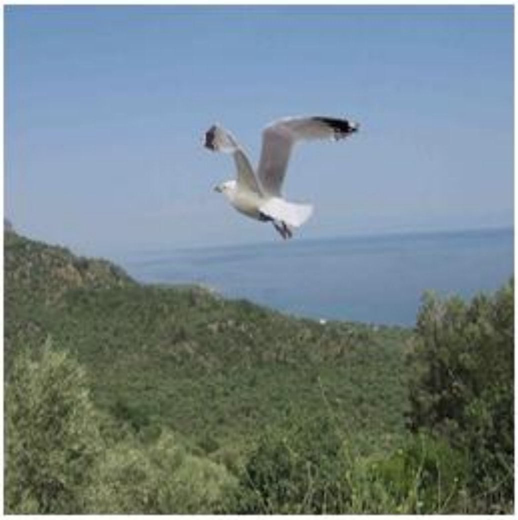


Fig.8(b). Extracted Secrete Image by using 16×16

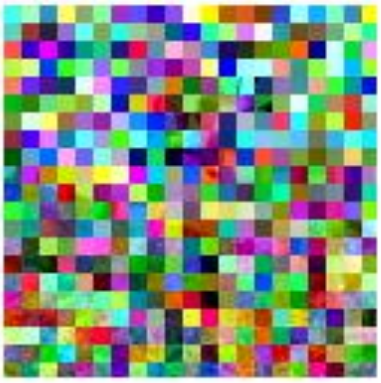


Fig.9.Recovered secret image using a wrong key

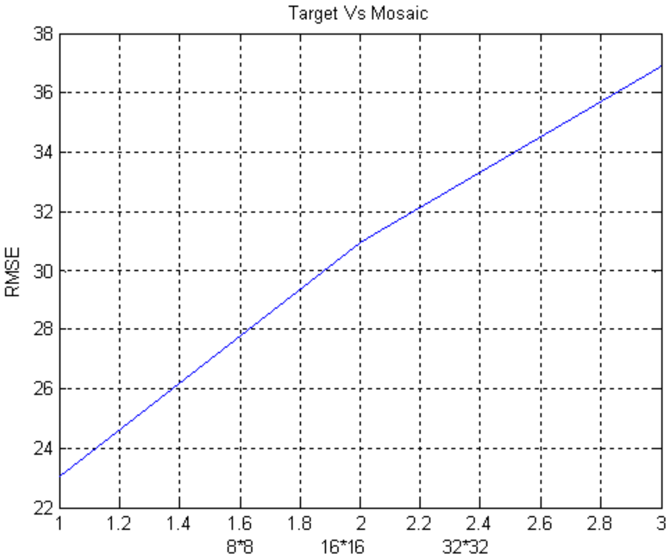


Fig.10. arget image Vs mosaic

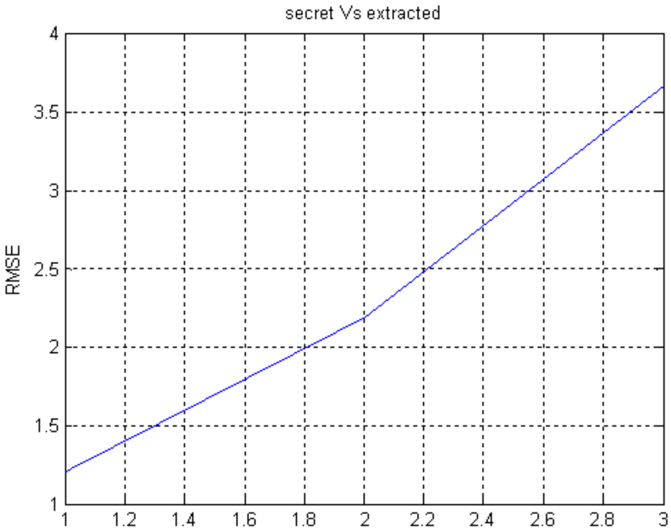


Fig.11. RMSE for secret image Vs extracted image

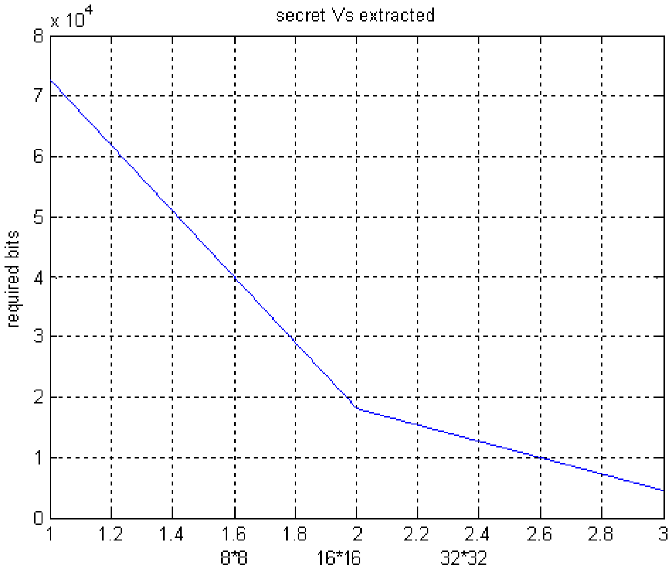


Fig.12. required bits for secret image Vs extracted image

CONCLUSION

Another safe picture transmission strategy has been proposed, which can make important mosaic pictures as well as can change a mystery picture into a mosaic one with similar information measure for use as a cover of the mystery picture. By the utilization of appropriate pixel shading changes and also a dexterous plan for taking care of floods and undercurrents in the changed over estimations of the pixels' hues, mystery piece unmistakable mosaic pictures with high visual likenesses to self-assertively chose target pictures can be made with no need of an objective picture database. Additionally, the first mystery pictures can be recuperated about losslessly from the made mosaic pictures. Great exploratory outcomes have demonstrated the attainability of the proposed technique. Future examinations might be coordinated to applying the proposed strategy to pictures of shading models other than the RGB.

REFRENCES

[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 modi-fication: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7,

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

[16] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13,2768–2786, 2007.