International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 12 6478 - 6484

A Review on Image mosaicing for secure Transmission of University Exam Question Paper

Miss. Suchita N. Sangvikar
PG student: dept. of Electronics
Savitribai Phule Women's Engineering College,
Aurangabad, India
suchitasangvikar@gmail.com

Mr. P. R.Thorat
Assistant Professor, dept. of Electronics
Savitribai Phule Women's Engineering College,
Aurangabad, India
thorat.popat.r@gmail.com

***Abstract*—**The rapid spread of the digital world nowadays which is powered by ever faster system demands greater speed and security. Real time to secure an image is a challenging task due to the processing time and computational requirement for RGB image. So, to cope with these concerns, many innovative techniques of image processing for data hiding are required. In this paper new data hiding scheme is proposed which is known as image mosaicing. Image mosaicing is the process of merging split images to produce a single and complete image of the document. For this technique two input images are required one is secret image and second is target image, by merging these two a new image is made called as a mosaic image. So, the creation of mosaic image and lossless recovery of secret input image for question paper security is presented in this paper.

Keywords- *mosaic image, Color transformation, secure image transmission, image encryption, data hiding.*

*****

I. INTRODUCTION

As the world changes, technology is changing rapidly. Network technology in the domain of progress, relatively large amounts of multimedia information is broadcast on the Internet with ease. Such as government, military, banking and other secure data, taken from space and satellites and commercially important document geographic image as confidential data are transmitted over the Internet. The use of confidential information, while we need more secure information hiding technique. Currently, images from different sources is often used and such online personal photo album, secret Enterprise archives, document storage systems, medical imaging systems, and military image as the database for different applications are transmitted via the Internet . During all communication must be protected from the limestone, the image that usually contain private or confidential information. Recently, many methods of the two most common ways are hidden image encryption and data, image transmission, have been proposed for protecting. Image encryption based on confusion and diffusion properties of Shannon to obtain an encrypted image, such as high redundancy and a strong spatial relationship of the natural property of an image is a technique that uses [1] - [7]. He / she is the right key, until it no secret image that can receive an encrypted image is a noisy image.

Therefore, the method for hiding data in images is a major issue in a single image message is difficult to add a large amount of data. With one of the same size in a cover image he wants to hide a secret image, especially, the secret image in advance should be highly compressed. For example, at a rate of 0.5 bits per pixels displayed for a data hiding method, with 8 bits per pixel image a secret to be hidden in the cover image with a minimum rate of 93.75% should be compressed. However, there are serious distortions with no allowance valuable, or more medical images such that the military image, legal documents, sent for many applications, such as data compression processing is usually impractical.

In this paper, a safe, a new technique for broadcasting images the same size in the image of Moses as a means of changing a secret image and a preselected target image is looking like that is proposed. Conversion process is controlled by a secret key, and only a person with the key image of Moses nearly losslessly can recover the secret image. The proposed method Lai and is inspired by Tsai [8], in which secret-Part-called visual image of Moses, a new type of computer art image was proposed. Mosaic image to a database called preselected target image in disguise to another image of a hidden image is the result of the sequence of pieces. Moses selected image of the target image, which can be quite similar but Lai Tsai's an obvious weakness [8] requires a large image database. Using the method, the user free to use as the target image of his / her favorite images is not allowed to select. While keeping its merit this method to remove this weakness in the study that is required, it is the same size that a secret piece of visual images of Moses in a secret image change a new method that aims to create a database without the need for any free target selected visual appearance of the image. A source image that contains small pieces of secret-Part-called visual image of Moses and a new type of art image, Lai Tsai has proposed in this study. Moses seen such kind of image, of a source image can see all the pieces, but pieces observer looks like the source image can not figure out what that size, so small and in position , so constant. Therefore, the source image component pieces are available for all observers, however, results secret law can be said to be included in the image. Moses and the results have been kept secret-Part-visual images, is the reason why. It includes three phases. The database is built. The second phase of Moses image composition and the third image of Moses decryption.

As an example, Figure 1 (a) shows a secret image in the figure shows an example of the proposed method, (b) a target image and Figure (c) made secret-piece mosaic shown represents the image shows (a) and (b).

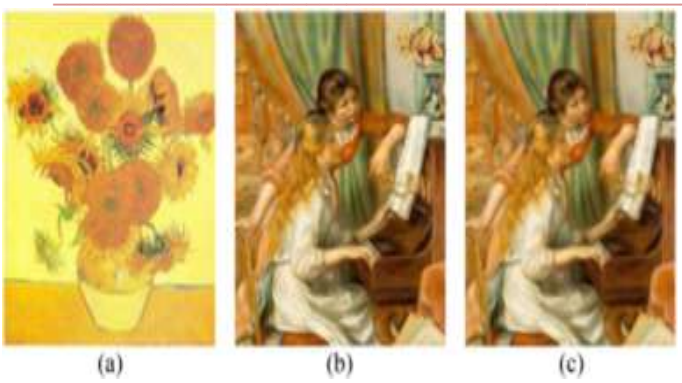

Figure 1..One example of proposed method. (a) Secret image. (b) Target image. (c) Secret mosaic image created from (a) and (b)

A target image is chosen arbitrarily, since, in particular the secret image by the color variations according to a similarity criterion, similar blocks in the target image is called the target block are fitted in the images are divided into pieces called tiles, which are rectangular. Next, the characteristic color of each tile image of the target image looks like, resulting in a mosaic image, the target image corresponding to the target block that is transformed. The relevant plans, resulting in a mosaic image of the original secret image is proposed to conduct virtually lossless recovery. A meaningful mosaic image as meaningless noise creates images that contrast with the image encryption method, the new method is proposed that is created. A data hiding method in a cover image of a highly compressed version of the image must hide the secret, the secret image and the cover image is the same data volume Also, the proposed method, one without compression disguising a secret image in the mosaic image change are [8].

A. Necessity

Privacy and anonymity on the Internet is a concern for most people. The two sides to communicate secretly and covertly allows image steganography. The internal actions to safely blow the whistle to some morally conscious people allows; This is the message as a digital watermark for copyright protection on digital files using allows. The other main use of a high level of image steganography or international governments is to transport the top secret documents. Image steganography many legitimate uses, it can also be quite nefarious. The terrorists and to communicate secretly and safely rely on covert operations by the other organizations compromised machines to be used by hackers to send viruses and trojans can.

B. Theme

Secret image mosaic image creation and recovery: The proposed method consists of two main stages. The first phase includes four stages: a pre-selected target the secret image in the image of the target block tile images fittings; Secret image characteristic change in the color of each tile image in the target image to be that of the target block; With respect to its corresponding target block with the minimum RMSE value for each tile image in a direction of rotation; Secret image mosaic created for the future recovery of relevant information in image embedding. The second phase includes two stages: a mosaic image of the hidden image recovery extract embedded information; Fix the image using the extracted information secret. If the target image from a database in order to avoid the difficulty of selecting the image, can be chosen arbitrarily. Security is also enhanced in comparison to the former method.

II. LITERATURE REVIEW

Literature Survey is the most important step in the software development process. Tools developed before the time factor, the economy and the company is required to determine power. These things are satisfied, then the next step is to develop the operating system and language tools can be used, which is to determine. Programmer tools to start building the programmer needs a lot of external support. The support from the book or websites, can be obtained from senior programmer. Before the construction of the idea of the system for the development of the proposed system are taken into account. In this chapter we present the online examination system, the university exam pattern, image encryption are focused on different systems.

A. Existing online examination system

Testing with large and small people today to go through trials, once the issue is being faced. Moreover, fair and open trial system properties. It is also the best way to measure academic performance. The examinations can not be ignored, which costs society less come from. In addition to testing different conference each year, taking the combined test are so many people, it will be a considerable figure. Today the Internet is nothing that could not. , Read news and happening in the most recent example of online classes as well as awed everyone who orders online, online restaurants, online bidding, followed by, etc. shopping, e-shops to browse. In the future, neither students nor teachers to teach classes will be required to go to school will be required to go to school. Lessons through online learning and online classes will be held. The problem arises because the exam. Online examination system is the answer to the problem. In the Internet age, an online examination system is necessary. Online exam have neither the time nor the place of examination is limited by. During the test in accordance with the progress of the lessons can be arranged. Since tests are examined by computer at the same time, test time and cost saved is a manual exam. Based on the properties of the Internet, online testing for students and for teachers to revise the questions online website creation with the setting and management of online examination system concept is designed for.

Online examinations are convenient and fast. The current concern is not cheated through fraud. Depending on the formulation test questions. Exam questions are tough and prepared with care. Test in multiple choice format, questions are selected at random. All students have the same question, but the question is a different order. The order of questions is different on each computer, the cause is reduced to cheat students. Cheating in exams is unacceptable. So, technically to overcome fraud or deception for the purpose of alleviating the students is the biggest challenge for the online exam.

Web-based survey and survey forms are advantages to both administrators and respondents.

The system for the number of students of graduation and post-graduation admissions process is followed by various institutions as well as the online examination system in India is carried out nowadays in almost every public and private sectors goes. Online examination system is now in the banking sector, such as the recruitment of probationary officers and clerks in various competitive examinations for recruitment purpose of getting along with the selection of employees to different positions in the UPSC exam for Maharashtra Public Service Commission, the Commission on railway, various insurance companies etc.

B. University Examination Pattern in India

The online exam system discussed in above section is a type of objective based exam pattern. That means the exam consists of multiple type objective questions for which students have to answer the questions just by clicking one option out of four or five options. But this type of exam is not taking place in university exams and secondary and higher secondary school certificate exams. These exams are totally based on descriptive type of question in which students have to write answers of the questions. Students write the answers on answer sheets provided them by seeing question on question paper. In this system university, state board, central board, technical education board sends the question papers to respective colleges or schools. Though they do this procedure by maintaining the security there are still chances to leak the question papers. Unfortunately this leakage of question paper has actually happened more times. Manual sending of question papers to each college is a herculean task and involves risk of paper leaks.

The solution to solve the above problem is to send the question papers online to the institutes instead of manual sending of question papers. The online process will ensure confidentiality and security of question papers. Some universities in India like Uttar Pradesh Technical University (UPTU), Visveswaraya Institute of Technology (VIT), Karnataka, have first adopted the process of sending online question papers to corresponding colleges. But now almost maximum universities, management colleges, technical universities across the country started this process and thereby trying to maintain confidentiality and security of question papers. The system when put into place helps in saving time and money. The online sending of question papers to the colleges will be based on online question paper delivery system (QPDS). The process will be connected to the National Mission on Education through Information and Communication Technology (ICT) sponsored by the ministry of human resource and development.

University officials working on the online examination reform explained that through QPDS, question papers will be send on the basis of number of examination forms received by the university and total number of students enrolled in a particular college. The question papers will reach the college 45 minutes before the commencement of examination. Colleges can take the print outs of the question papers once it reaches on the centre login. Only principal, examination superintendent and system administrator would have access to the unique color coded identity. Each question paper must have a different color identity.

Even though the online sending of question papers seems to be confidential the hacker may breaks this security. Many hackers breech inside a network and steal passwords, which will be used or sold, perform industrial espionage, or commit simple misuse. Hacking is to steal ones secret by breaking security. The chances to steal question paper while sending online is easy for hacker. So, again the problem of paper leak arises. This can be prevented by overlapping the actual paper with another image. Thus by making use of proper methods of image encryption, data hiding and secure recovery of original information we can maintain secrecy of our important document.

C. Different existing systems for image encryption

1) With four multi-pixel block size encoding structure for general use by- visual cryptography:

Multi-pixel encoding for each run more than one pixel can encode the visual cryptography is an emerging method. However, in reality its encoding efficiency is still low. The variable number of pixels for each run, which can encode a novel multi-pixel encoding represents. Without the proposed extension of the pixel structure and colorful images for general use, can work well.

2) Partial color visual cryptography:

Visual Cryptography random binary pattern shares a secret binary image encodes. This graph colorings using extended visual cryptography shares binary images to produce meaningful as was recently proposed, but the visual quality is poor. A novel technique named halftone half toning through visual cryptography is proposed to achieve visual cryptography.

3) Print and scan applications-visual cryptography:

Yan et al. They have found a way of properly aligning the shares, which proposed a plan. They came up with two ways: First, they put a mark next to the shares and the shares that are covered by the mark. The first technology stocks and reconstructed image. Secondly, they make use of the extended visual cryptography scheme put marks in stocks. The two technologies work in the spatial domain. The drawback of these methods for unauthorized alignment marks are visible and thus easily (the first method) and (second method) can be removed by localized crop the image changes.

4) Joint Visual Cryptography and Watermarking:

In this technique both halftone watermarking and visual cryptography involve a hidden secret image. However, their concepts are different. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in a single halftone image while preserving the quality of the watermarked halftone image.

- Drawbacks of existing system
  - A main issue of all these methods for hiding data in images is the difficulty to embed a large amount of message data into a single image.
  - Most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between

adjacent pixels are often destructed to become noticeable artifacts.

III. SYSTEM DEVELOPMENT

A. *Flow diagram of the Proposed Method*

The flow diagram shown in Figure 2, the proposed method comprises two main steps:

1) Moses' image creation and
2) to recover the secret image.

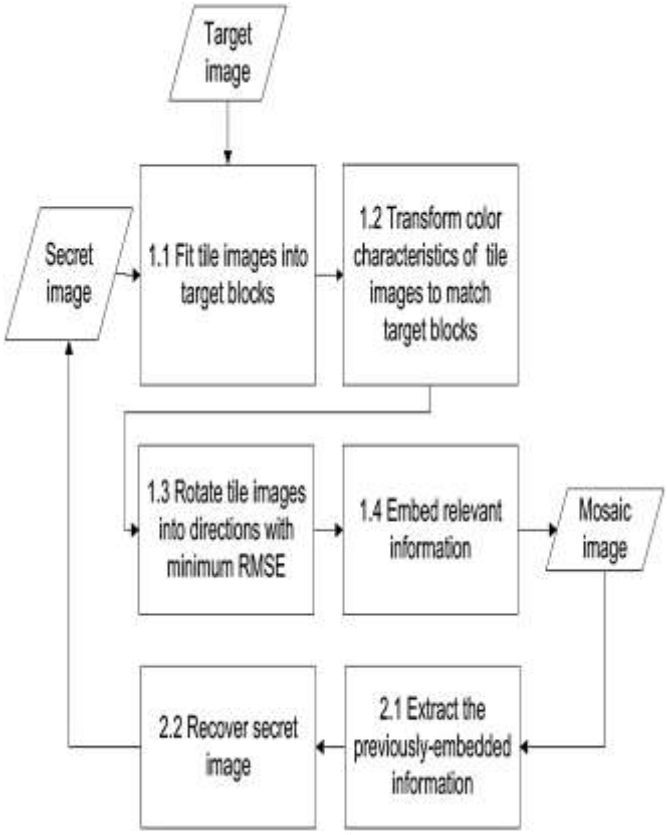

Figure 2. Flow diagram of the proposed method.

In the first phase of a mosaic image based on color variations according to a similarity criterion with color correction consists of an input secret image fragments, which has yielded. Step four steps include:

1) The goal of the chosen target image block fitting tile images of the secret image;
2) secret image characteristic change in the color of each tile image in the target image to be that of the target block;
3) with respect to its corresponding target block with the minimum RMSE value for each tile image in a direction of rotation; And
4) Secret image mosaic created for the future recovery of relevant information embedded in the image. In the second phase, the embedded information generated mosaic image almost losslessly to recover the secret image is adjusted.

Phase two phases include:

• Mosaic image recovery from the secret image for extracting embedded information, and
• Using information extracted recover secret image.

B. *Ideas of Mosaic Image Generation*

1. Color Transformations between Blocks

The method proposed in the first phase of the secret image in a chosen target image in each tile image T is fitted into a target block B. T and B color characteristics are different from each other, so they look alike to make the main issue here is how to change their color distribution. Reinhard et al. [10] lαβ color space that can be of another color characteristic of an image converts a color transfer scheme proposed in this aspect. The idea for this issue is an answer and instead lαβ a secret image of the RGB color space for the collection of basic information needed to reduce the amount of used, except that the paper is adopted.

More specifically, the T and B two pixel set $\{p_1, p_2, \ldots$ as described . , $p_n\}$ and $\{p'_1, p'_2, \ldots$, Respectively: $p'_n\}$. Let each one p_i disturbances of color (r_i, g_i, b_i) and be marked with $(r'_i g'_i b'_i)$. First, we have three color channels R, G, and B in each of the means, and respectively T and B, calculate the standard deviation. After that, we the new color values (r''_i, g''_i, b''_i)T for each p_i calculated by

$$c_i'' = q_c (c_i - \mu_c) + \mu_c' \quad (1) [8].$$

The $q_c = \sigma_c' / \sigma_c$ standard deviation quotient and c = r, g, or b. It means new paint and tile the resulting image T 'variance, respectively, are similar to those of B that can be easily verified. Mess with people's basic color values (r_i, g_i, b_i) to calculate $(r'_i g'_i b'_i)$, we use the inverse of the following formula (1):

$$c_i = (1/ q_c) (c_i'' - \mu_c') + \mu_c \quad (2)$$

Furthermore, we recover the original secret image for use at a later stage new tile image T' made about the information embedded in the mosaic image is enough. This theoretically we calculate p_i to the original pixel value (2) can use. However, the mean and standard deviation values in the formula are the real numbers, and the resulting mosaic image, the actual number, with many points is impractical for each embedding. Therefore, we represent the values of the relevant parameters to limit the number of bits (1) and (2). In particular, we have for each color channel, with its value in the range of 0 to 255 for 8 bits for each of T and B means allow, and the standard deviation quotient q_c (1) in with price range of 0.1 to 12.8 to 7 bits. That means each 255 of0 nearest value in the range to be changed, and the nearest value in the range of 0.1 to 12.8 for each q_c is to be changed. Otherwise can not be recovered by the original pixel value is returned, because we are not allowed to be q_c 0 (2) the reason for the 1 / q_c (2) $q_c = 0$ is not defined.

2. Designed to fit better with smaller RMSE value target block and a rotating selection of blocks:

To change the color attribute of a tile image T is an issue for each T to select a suitable B, as described above, a similar target to that of block B can be. For this, we specifically for each t B to select the most similar block as a measure of the standard deviation in the use of colors, tile images We all like to form a view, dipping, and For all target blocks form, S_{target}, the standard deviation of the average values of the three color channels. So, we have so on, S_{target} dipping in the first dipping in the second in the first fit S_{target} second fit in, and.

Having chosen not to fit the end use of the four directions with respect to B T with a rotated version of the minimum root 'mean square error (RMSE) value, which yields one of four directions , 0^o, 90^o, 180^o, and 270^o, the B.

3. Handling Overflows / Underflows color change

As previously described process is conducted after the color change, new tile image T' may have some pixel values overflows or underflows. To tackle this problem, we may be people of non overflow or underflow and the recovery of non-use value differences persist as to record changes in such values. In particular, we do not have to be 255 to 255 small 't change the transformed pixel values, and not all of them are big minus 0. Next, we changed the original pixel values and survive as more people calculating differences between not record them as part of the information associated with. Overflow / underflows up with all the pixel values are converted to 255 or 0 since Accordingly, only 255 or 0 pixel values which are bound, however, during the subsequent recovery overflow / underflow with values different from those that can not be. To remedy this, we can be 0 as well as they are obliged to record the pixel values that define the escape.

However, as (1), possible residual values are unknown limits is seen, and it should be used to record a residual that causes the problem of deciding how many bits can be. To solve this problem, we untransformed color space instead of turning a residual value is recorded. That is why we first calculate the following two formulas, using the smallest possible color value Cs (c = R, G, or B) that is larger than 255 t, is the T the largest possible value in the short C_L 0, respectively, after the color change process has been conducted.

Next, for an untransformed value c_i which yields an overflow after the color transformation, we compute its residual as $| c_i - c_S |$; and for c_i which yields an underflow, we compute its residual as $| c_L - c_i |$. Then, the possible values of the residuals of c_i will all lie in the range of 0 to 255 as can be verified. Consequently, we can simply record each of them with 8bits. 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.

4. The mosaic image for image recovery by embedding secret information secret in order to fix the image, we have to embed the mosaic image information relevant recovery. Block B is mapped to target a tile image T to fix the necessary information: B 1) index; 2) T is the optimal rotation angle; 3) T and B and the standard deviation of all color channels of quotients means little; And 4) overflow / underflow survived. A tile image T to recover form data item as a five component bit stream are integrated.

C. Algorithms:-

Based on the above discussion and secret mosaic image building elaborate algorithms for image recovery algorithms 1 and 2, respectively, as now can be described.

1) Algorithm 1: Mosaic Image Construction Input: a secret image S, a target image T, and a secret key K. Output: a secret-piece mosaic image appears F Steps:

- *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 $\{T_1, T_2, \ldots, T_n\}$ as well as the target image *T* into *n* target blocks $\{B_1, B_2, \ldots, B_n\}$with each T_i or B_i being of size N_T.

➢ Step 2: For the three color channels B_J The mean and standard deviation of each tile and each target image T_I Compute block (1) and (2); And through N and j = 1 through n = I 1 respectively T_I and B_J accordingly, the average standard deviation.

➢ Step 3: Sort the tile images in the set $S_{tile}= \{T_1, T_2, \ldots, T_n\}$ and the target blocks in the set $S_{target} = \{B_1, B_2, \ldots, B_n\}$according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted S_{tile} to those in the sorted S_{target} in a 1-to-1 manner; And form a mapping sequence, resulting in L tile images according to the index mapping reorder:
$T_1 \rightarrow B_{j1}$, $T_2 \rightarrow B_{j2}$, . . . , $T_n \rightarrow B_{jn}$.

➢ Step 4: L According to the tile images in the target blocks a mosaic image by fitting F Create.

- *Stage 2. performing color conversions between the tile images and the target blocks.*

➢ Step 5: With an index corresponding to a residual value of 256 entries, each with one count Create table TB, and each entry (note that each residual value will be in the range 0-255) for an initial value of zero assigned.

➢ Step 6: For each mapping $T_i \rightarrow B_{ji}$ in sequence *L*, represent the means μ_c and μ'_c of *T* and B_{ji}, respectively, by eight bits; and represent the standard deviation quotient q_c appearing in (1) by seven bits, where *c* = *r*, *g*, or *b*.

➢ Step 7: C = R, G, or B, by (1) a new value in c_i" change the C_I , C_I with the color value of each tile image mosaic image of F in T_I for each pixel manipulation, c_i" 255 is not smaller than or not it is greater than 0, then c_i" change 255 or 0, respectively be, pixel manipulation required to calculate the residual value, and is equal to 1 to re-count the index entry in the table T B increment count.

- *Stage 3: tile rotating images.*

➢ Step 8: After rotating directions in each of T_i with respect to its corresponding target block B_{ji} F tiles into each color image T_i RMSE values calculated $\theta = 0^o$, 90^o, 180 degrees and 270^o; And the smallest RMSE value in the optimal direction θ^o rotate Tiwari.

- *Stage 4.: Secret image recovery information embedding.*

➢ Step 9: first, the residual values calculated from the counting table to encode content using T B HT build a Huffman table.

➢ Step 10: 1) Index: Section 3.3 (d), as described in the mosaic image in F for each tile image T_i, is to encode data items, including the little-blocks in the way a bit to recover T_i B_{ji} stream Mi building blocks of the target; 2) optimal rotation angle of T_i θ °; 3) Ti and B_{ji} and belonging to all three color channels means of standard deviation quotients; And 4) for overflow bit sequence / step 9 encoded by the HT building in the Huffman table with T_i survived underflows.

➢ Step 11: Bit mount a total bit stream in order to form a raster scan all T_i M_i streams coherence in F; M't another bit stream to encrypt the secret key k Use the mount; And

[10] In contrast reversible mapping scheme proposed by M't embed F.

- Step 12: I create a bit stream including: M't to embed the iterations N_i 1) number; N_{pair} last visit pixel used in pairs 2) number; And 3) build the Huffman table HT to escape; And in step 11 use the same plan I bit stream embedded in the mosaic image f.

2) Algorithm 2: Secret image recovery
Input: A mosaic image *F* with *n* tile images $\{T_1, T_2, ...T_n\}$and the secret key *K*.
Output: S - secret image
Steps:

- *Stage 1: extract secret information image recovery.*

- Step 1: From [10] In a reverse version of the proposed plan by the bit stream I explain them to get out, and the following data items: 1) M't N_i number of iterations to be embedded; Pixel pairs used 2) the total number N_{pair} final journey; And 3) to avoid overflow or underflows the Huffman table for encoding HT values.
- Step 2: Use the same scheme in the final stage by using the values of Ni and N_{pair} Remove M't bit stream.
- Step 3: K. M'_t decrypt the bit stream at M_t.
- Step 4: respectively, in T_n through S n-to-be constructed tile images T_1 million through the M_1 mount decomposed into N-bit streams.
- Step 5: Explain Mi Tito received the following data items for each tile image: 1) B_{ji} index G ,F Tiwari same block; 2) optimal rotation angle of Ti θ °; 3) T_i and B_{ji} all color channels and the related standard deviation quotients instruments; And 4) overflow / Huffman table decoded by HT residual value underflow at T_I.

- *Stage 2: Secret image recover.*

- Step 6: Following the steps desired by the secret image S, i = 1 through N, in a raster scan order, one after the recovery of tile images T_I: 1) block to rotate in the opposite direction, ie indexed by G B_{ji}, F ° θ and Tito resulting in optimum angle through the block material to form an initial tile image T_I fit; 2) Ti recover the original pixel values derived instrument and related to the use of standard deviation quotients; 3) removal of the mean, standard deviation quotients use, and (5) two parameters to calculate C_S and C_L; 4) Tito overflows or underflows, respectively, which indicate that there has been to detect pixels with values of 0 to 255 or scan; 5) found that the residual values for the respective values of pixels adding C_S or C_L; And 6) a final tile image T_I, take the results as a result of which the final pixel values.
- Step 7: output as desired to form the secret image S from the last tile images.

Thus authors Lai and Tsai proposed a new type of computer art image, called secret-fragment-visible mosaic image, which is the result of random rearrangement of the fragments of a secret image in disguise of another image called *target image*, creating exactly an effect of image steganography[8].

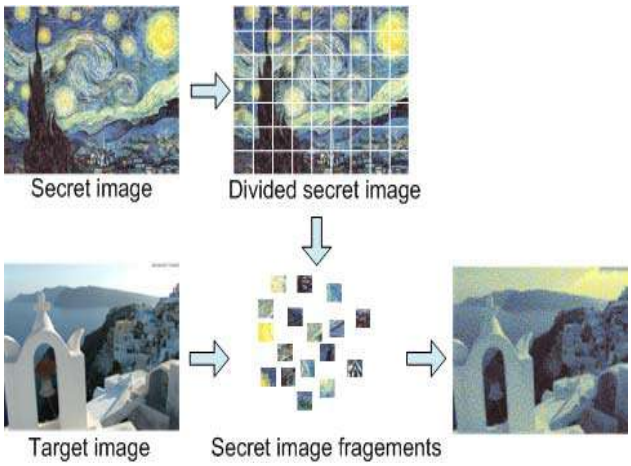

Figure 3. Show-piece mosaic depicting the image of the mystery of creation

It is clear from Figure 3, a small rectangular pieces of the secret image in the "cut" is the first, and a uniform color distribution with a target image is selected from a database. Then, the pieces of a mosaic image with the presence of the target yield a Stego image to fit into the block controlled by a key are arranged in a random fashion. Stego image appearance preserves the secret image pieces, but none of the original secret image can figure out what that looks like. The method is a new way to preserve secret images.

IV. CONCLUSION

We manufacture mosaic image of the university system for the secure transmission of papers are supposed to develop. Hide Paper Input Paper image with another image of the same size needs to be covered. So, a new secure image transmission method can make meaningful mosaic picture, but also the mystery of the image used as a camouflage for the size of the same data with a secret image into a mosaic one can change, not has only been proposed. The receiver is the decryption key, the mosaic image of the original input when it can not decode the secret papers. With proper pixel color changes with very high visual similarity pixels' color, mystery-piece mosaic images appear to deal with changed values are swept and underflows target by using an efficient plan can be created with images arbitrarily selected image to the target database does not have any. The proposed system to improve the visual quality of the image and the human visual and statistical attack, attack opposition may be focused on reducing. Also, the original secret images created almost losslessly mosaic images can be cured. This mosaic image creation and image-recovery system to send secret paper would be helpful in maintaining the secrecy and confidentiality. Now the challenge is to prevent the leakage of question paper that our objective is to achieve the performance of this system.

A. *Advantages*

1) User target image for use as freely his / her favorite images are not allowed to choose. So this method of

keeping their ability to overcome this weakness in the study is desired.

2) It is aimed to design a new method that can transform a secret image into a secret fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.
3) Only the receiver who has the key can decode the secret image. However, an eavesdropper who does not have the key may still try all possible permutations of the tile images in the mosaic image to get the secret image back.
4) The image quality is high comparing to the existing system, by placing image into blank created image.
5) Tile image placing are compared with the entire target image and choose the perfect match for the tile.

B. Disadvantages

1) The proposed method offers a range of possible input target image size to match those of latent images. We have to select the target picture is a very big secret image, but only small, particularly if any of the selected target image in order to match the size of the secret image mosaic image must be enlarged before construction, and made mosaic The image will be blurred.
2) The major difficulty of this method is the maintenance of large database. We also feature h and histogram for each image in the database to calculate, because these values to store memory. Greedy search algorithm to find the similarities between aand more time is taken. So the computational complexity will be much greater.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.
[2] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21, no. 3, pp. 749–761, 2004.
[3] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," *Chaos Solit. Fract.*, vol. 24, no. 3, pp. 759–765, 2005.
[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solit. Fract.*, vol. 32, no. 4, pp.1518–1529,2007.
[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos Solit. Fract.*, vol. 35, no. 2, pp. 408–419, 2008.
[6] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos based 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] I.J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding," *IEEE Trans. Inf. Forens. Secur.*, vol. 6, no. 3, pp. 936–945, Sep. 2011.
[9] 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.
[10] 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.