**SECURE IMAGE STEGANOGRAPHY SCHEME FOR INFORMATION HIDING**

**MINOR PROJECT I**

Submitted By:

**Abhi Rustagi (9916103144)**

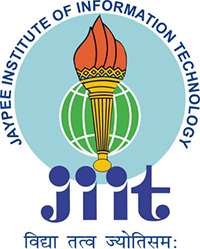
**Bhoomika Gupta (9916103121)**

**Srajan Ahuja (9916103111)**

**Vansh Jain (9916103191)**

Under the supervision of:

**Dr. Gyan Singh Yadav**

****

**Department of CSE/IT**

**Jaypee Institute of Information Technology, Noida**

**November, 2018**

**ACKNOWLEDGEMENT**

We would like to place on record our deep sense of gratitude to **Dr Gyan Singh Yadav**, Jaypee Institute of Information Technology, Noida, India for his generous guidance, help, useful suggestions, continuous encouragement and supervision throughout the course of present work.

**Signature of Students:**

Abhi Rustagi (9916103144)

Bhoomika Gupta (9916103121)

Vansh Jain (9916103191)

Srajan Ahuja (9916103111)

**Signature of Supervisor:**

Dr. Gyan Singh Yadav

**ABSTRACT**

A secure image transmission technique is proposed, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image.

Skillful techniques are designed to conduct the color transformation process so that the secret image recovered may be nearly lossless. A scheme of handling the overflows/underflows in the converted pixels’ color values by recording the color differences in the untransformed color space is also proposed.

The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme.

**TABLE OF CONTENTS**

Page no.

Acknowledgement  *ii*

Abstract *iii*

List of Figures *v*

List of tables *v*

Abbreviations and Nomenclature  *v*

**CHAPTER 1: INTRODUCTION 1**

* 1. Scope 1
  2. Purpose of the project 1
  3. Overview of the project 1

**CHAPTER 2: LITERATURE REVIEW/ BACKGROUND STUDY 2**

2.1 Steganography and Data Hiding 2

2.2 Mosaic Image 2

2.2.1 Secret Fragment Visible Mosaic Image 2

2.3 Summary of Research Papers 2

2.3.1 Research Paper 1 2

2.3.2 Research Paper 2 3

2.3.3 Research Paper 3 4

**CHAPTER 3: REQUIREMENT ANALYSIS 5**

3.1 Software 5

3.2 Hardware 5

3.3 Functional Requirements 5

3.4 Non-Functional Requirements 5

3.5 UML Diagram 6

**CHAPTER 4: DETAILED DESIGN 7**

4.1 Mosaic Creation 7

4.2 Secret Image Recovery 8

**CHAPTER 5: IMPLEMENTATIONS 11 CHAPTER 6: EXPERIMENTAL RESULTS AND ANALYSIS 12 CHAPTER 7: CONCLUSION AND FUTURE SCOPE 15 REFERENCES 16**

**LIST OF FIGURES**

**Figure**  **Title** **Page No**

1. Basic flow of Research paper 1 2
2. Basic flow of Research paper 2 3
3. Basic flow of Research paper 3 3
4. Use case diagram 4
5. Detail design 7
6. Implementation 8
7. Gantt Chart 10

**LIST OF TABLES**

**Table Title Page No**

1. Table 1: Hardware requirements 10
2. Table 2: Software requirements 10

**ABBREVIATIONS AND NOMENCLATURE**

* **SD** Standard Deviation
* **RMSE** Root Mean Square Error
* **PSNR** Peak Signal to Noise Ratio
* **HT** Huffman Table
* **T**  Target Image
* **K** Secret Key
* **F**  Mosaic Image
* **S**  Secret Image
* **n** Number of tile images

**CHAPTER 1 INTRODUCTION**

**1.1 Scope**

Now a days, various source images are transmitted and used through the internet for various applications, such as military applications, photography, document storages etc. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Currently there are two methods have been proposed for the transmissions, i.e. image encryption and data hiding.

**1.2 Purpose**

The purpose of the project is to perform image encryption to transmit the image securely so that no unauthorized user is able to decrypt the image. Its application is not only restricted for covert communication but also handles huge volume of data behind target images.

* 1. **Overview**

A secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image which is nearly lossless from the mosaic image. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image. The proposed method includes two main phases mosaic image creation and secret image recovery.

**CHAPTER 2: LITERATURE REVIEW/ BACKGROUND STUDY**

**2.1 Steganography and Data Hiding**

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images.

**2.2 Mosaic Images**

Mosaic is a type of artwork created by composing small pieces of materials, such as stone, glass, tile, etc. Creation of mosaic images by computer is a new research direction in recent years. Many methods have been proposed to create different types of mosaic images by computer.

**2.2.1 Secret Fragment Visible Mosaic Image**

A type of art image which contains small fragments of a given source image. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer.

**2.3 Summary of Research Papers**

**2.3.1 Research Paper 1: Secret-Fragment-Visible Mosaic Image– A New Computer Art and Its Application to Information Hiding**

A new type of computer art image called secret-fragment-visible mosaic image is proposed, which is created automatically by composing small fragments of a given image to become a target image in a mosaic form, achieving an effect of embedding the given image visibly but secretly in the resulting mosaic image. To create a mosaic image of this type from a given secret color image, the 3-D color

space is transformed into a new 1-D color scale, based on which a new image similarity measure is proposed for selecting from a database a target image that is the most similar to the given secret image. A fast-greedy search algorithm is used to find a similar tile image in the secret image to fit into each block in the target image. The information of the tile image fitting sequence is embedded into randomly-selected pixels in the created mosaic image using a secret key.

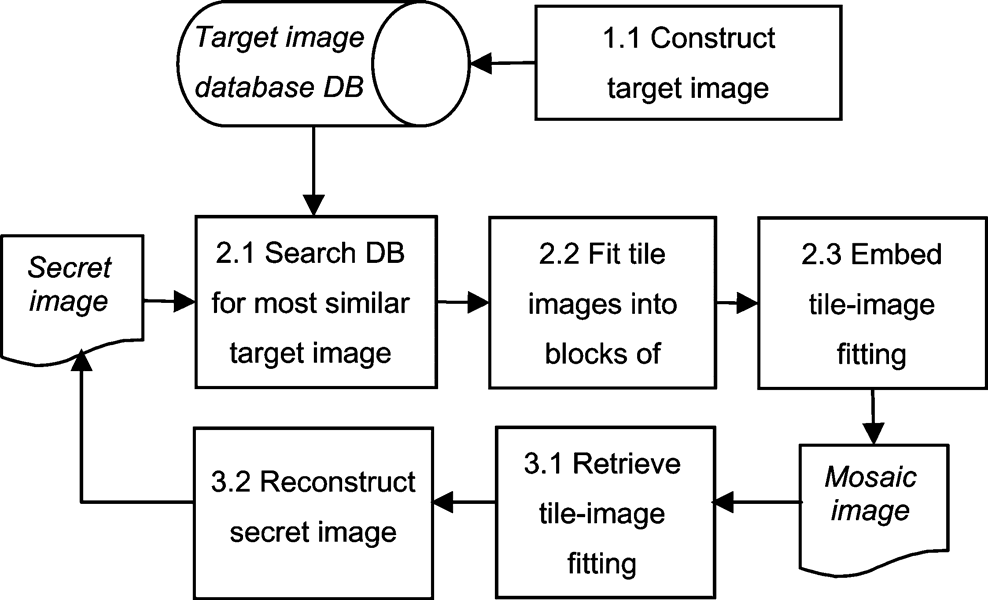


Figure 1: Flow diagram of research paper 1

**2.3.2** **Research Paper 2: A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations**

A secure image transmission technique transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. The color transformation process is conducted so that the secret image may be recovered is nearly lossless. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key.

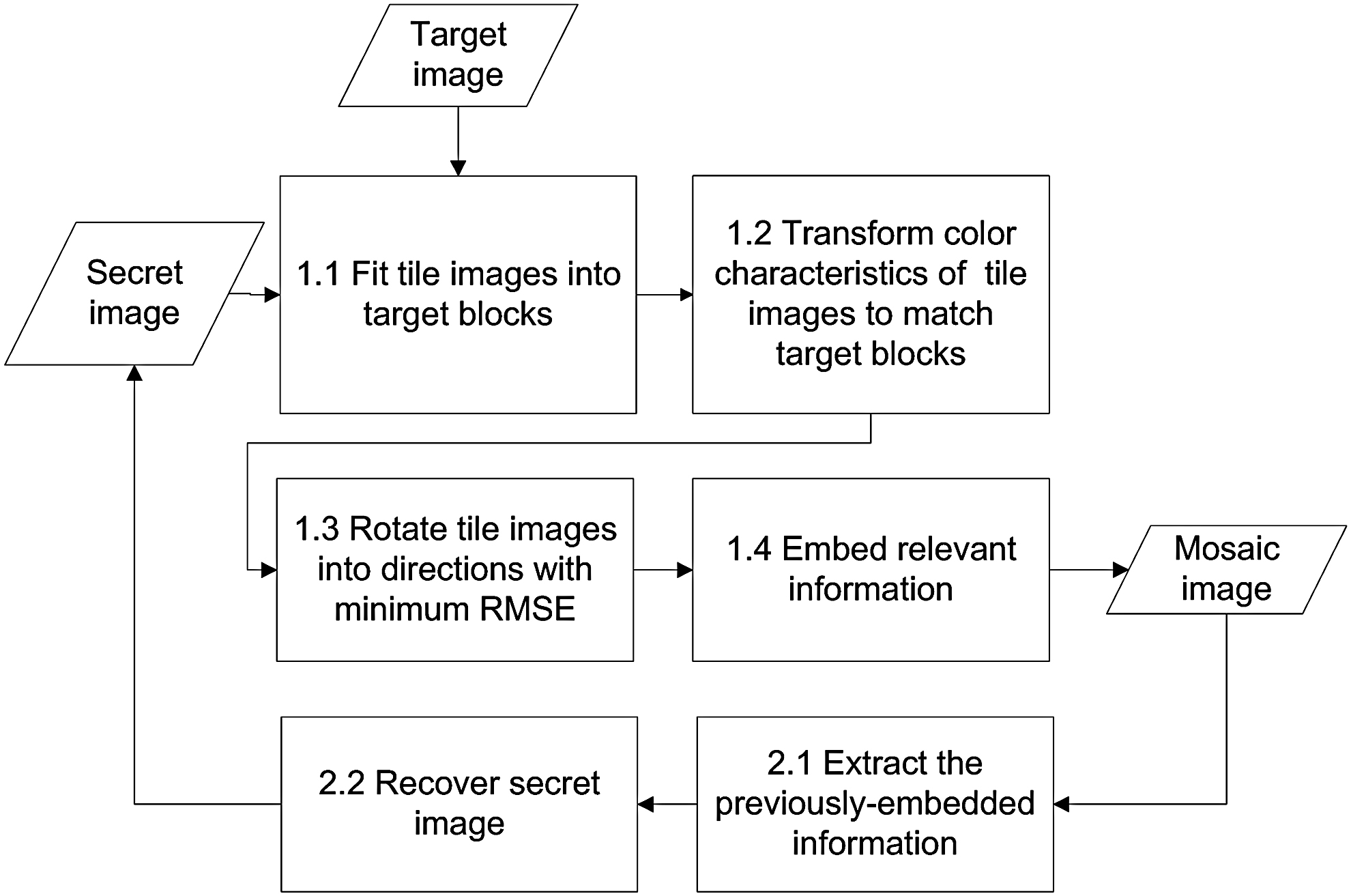


Figure 2: Flow diagram of research paper 2

**2.3.3 Research Paper 3: Genetic Algorithm based Mosaic Image Steganography for Enhanced Security**

A randomly selected image is used as the target. Genetic Algorithm (GA) is used to generate a mapping sequence for tile image hiding. This has resulted in better clarity in the retrieved secret image as well as reduction in computational complexity. The quality of original cover image remains preserved in spite of the embedded data image, thereby better security and robustness is assured. The mosaic image is yielded by dividing the secret image into fragments and embed these tile fragments into the target image based on the mapping sequence by GA and permuted the sequence again by KBRP with a key. The recovery of the secret image is by using the same key and the mapping sequence. This is found to be a lossless data hiding method.



Figure 3: Flow diagram for research paper 3

**CHAPTER 3: REQUIREMENT ANALYSIS**

**3.1 Hardware Requirements:**

|  |  |
| --- | --- |
| System | Pentium IV 2.4 GHz & Above. |
| Hard Disk | 40 GB & Above. |
| Monitor | 15 VGA Color. |
| RAM | 2 GB and above. |

Table 1

**3.2 Software Requirements:**

|  |  |
| --- | --- |
| Operating system | Windows 7 or above. |
| Coding Language | MATLAB |
| Tool | MATLAB |

Table 2

* 1. **Functional Requirements**
* **Encryption**
  + - * Secret Image Selection
      * Target Image Selection
      * Pre -Processing of Images
      * Embedding recovery Information
      * Mosaic Image Creation
* **Decryption**
  + - * Decryption Image Selection
      * Retrieving Image Recovery Information
      * Secret Image Recovery
  1. **Non-Functional Requirements**
     + Secure
     + Reliable
     + Data Integrity
     + Robustness
     + Testability
  2. **UML Diagram**

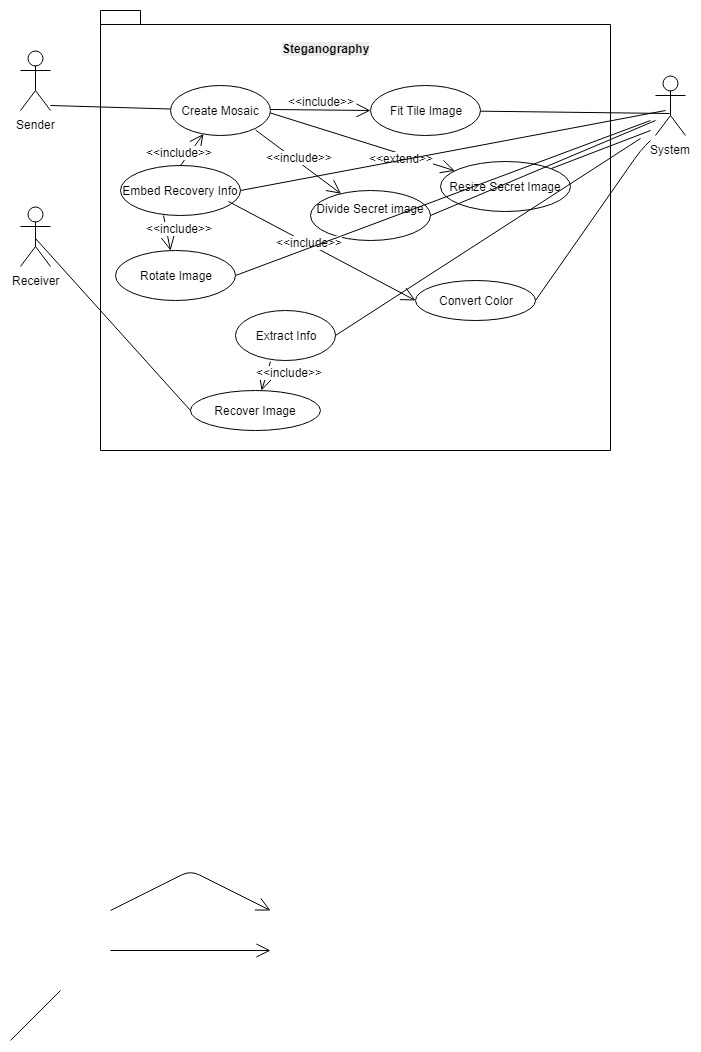


Figure 4: Use Case Diagram

**CHAPTER 4: DETAILED DESIGN**

**4.1 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*.

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 as well as the target image *T* into *n* target blocks with each *T*i or *B*i being of size *N*T .

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

Step 3. Sort the tile images in the set and the target blocks in the set *S*target 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 reorder the mappings according to the indices of the tile images.

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

Step 5. Create a counting table TBwith 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 in sequence *L*, represent the means μc and μ’c of *T* i and *B*ji , respectively, by eight bits; and represent the standard deviation quotient *q*c appearing in (3) by seven bits, where *c*=*r*, *g*, or *b*.

(3)

Step 7. For each pixel *p*i in each tile image *T*i of mosaic image *F* with color value *c*i where *c* = *r*, *g*, or *b*, transform *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 *R*i for pixel *p*i 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 *R*i .

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

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 *T*i in mosaic image *F*, construct a bit stream *M*i for recovering *T*i, including the bit-segments which encode the data items of:

1. the index of the corresponding target block *B*ji;
2. the optimal rotation angle θ° of *T*i;
3. the means of *T*i and *B*ji and the related standard deviation quotients of all three- color channels
4. the bit sequence for overflows/underflows with residuals in *T* i encoded by the Huffman table *HT* constructed in Step 9.

Step 11. Concatenate the bit streams *M*i of all *T*i in *F* in a raster-scan order to form a total bit stream *M*t; use the secret key *K* to encrypt *M*t into another bit stream *M’*t ; and embed *M’*t into *F* by the reversible contrast mapping scheme.

Step 12. Construct a bit stream *I* including:

1. the number of conducted iterations *N*i for embedding *M*′t;
2. the number of pixel pairs *N*pair 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.

**4.2 Secret Image Recovery**

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

Step 1. Extract from *F* the bit streams *I* by a reverse version of the scheme and decode them to obtain the following data items:

1) the number of iterations *N* i for embedding *M ‘*t

2) the total number of used pixel pairs *N*pair in the last iteration

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 *N* i and *N*pair by the same scheme used in the last step.

Step 3. Decrypt the bit stream *M’*t into *M*t by *K*.

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

Step 5. Decode *M* i for each tile image *T* i to obtain the following data items:

1) the index *j*i of the block *B*ji in *F* corresponding to *T* i

2) the optimal rotation angle θ° of *T*i

3) the means of *T*i and *B*ji and the related standard deviation quotients of all color channels

4) the overflow/underflow residual values in *T* i decoded by the Huffman table *HT*.

Step 6. Recover one by one in a raster-scan order the tile images *T* i , *i* = 1 through *n*, of the desired secret image *S* by the following steps.

1) rotate in the reverse direction the block indexed by *j*i, namely *B*ji, in *F* through the optimal angle θ° and fit the resulting block content into *T*i to form an *initial* tile image *T* i

2) use the extracted means and related standard deviation quotients to recover the original pixel values in *T*i according to (4)

(4)

3) use the extracted means, standard deviation quotients, and (5) to compute the two parameters *c*S and *c*L

(5)

4) scan *T* i to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there

5) add respectively the values *c*S or *c*L to the corresponding residual values of the found pixels

6)take the results as the final pixel values, resulting in a *final* tile image *T* i .

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



Figure 5: Flow of the program

**CHAPTER 5: IMPLEMENTATION**

In this section, we have described the tools used in this model and their purpose.

**Tools**

MATLAB® is a high-level technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numerical computation. Using MATLAB, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Java.

The version of MATLAB used in the project is MATLAB R2018a.

* **main\_gui.m**: MAIN\_GUI, by itself, creates a new MAIN\_GUI or raises the existing singleton. MAIN\_GUI('CALLBACK',hObject,eventData,handles,...) calls the local function named CALLBACK in MAIN\_GUI.M with the given input arguments. MAIN\_GUI('Property','Value',...) creates a new MAIN\_GUI or raises the existing singleton. Starting from the left, property value pairs are applied to the GUI before main\_gui\_OpeningFcn gets called. An unrecognized property name or invalid value makes property application stop. All inputs are passed to main\_gui\_OpeningFcn via varargin.
* **Rmse.m:** rmse.m is a function that calculates rmse values for all r, g, b colour values.
* **Decrypt.m:** Creates GUI for decryption of the image and carries out decryption. GUI is created on the same way GUI for main\_gui.m is created.
* **keygen.**m: A function that creates and embeds a key at the time of encryption of the process. In this process the image matrix column and row values are shifted based on the private key and generate key. The private key is given by users and the generated key is made by the given the image based on its size.





Figure 6: Flow of the program

**CHAPTER 6: EXPERIMENTAL RESULTS AND ANALYSIS**

The project was tested on various image samples and the following results were obtained:

**6.1 Encryption**

* Pre-processing removes noise from both the target image and the secret image.

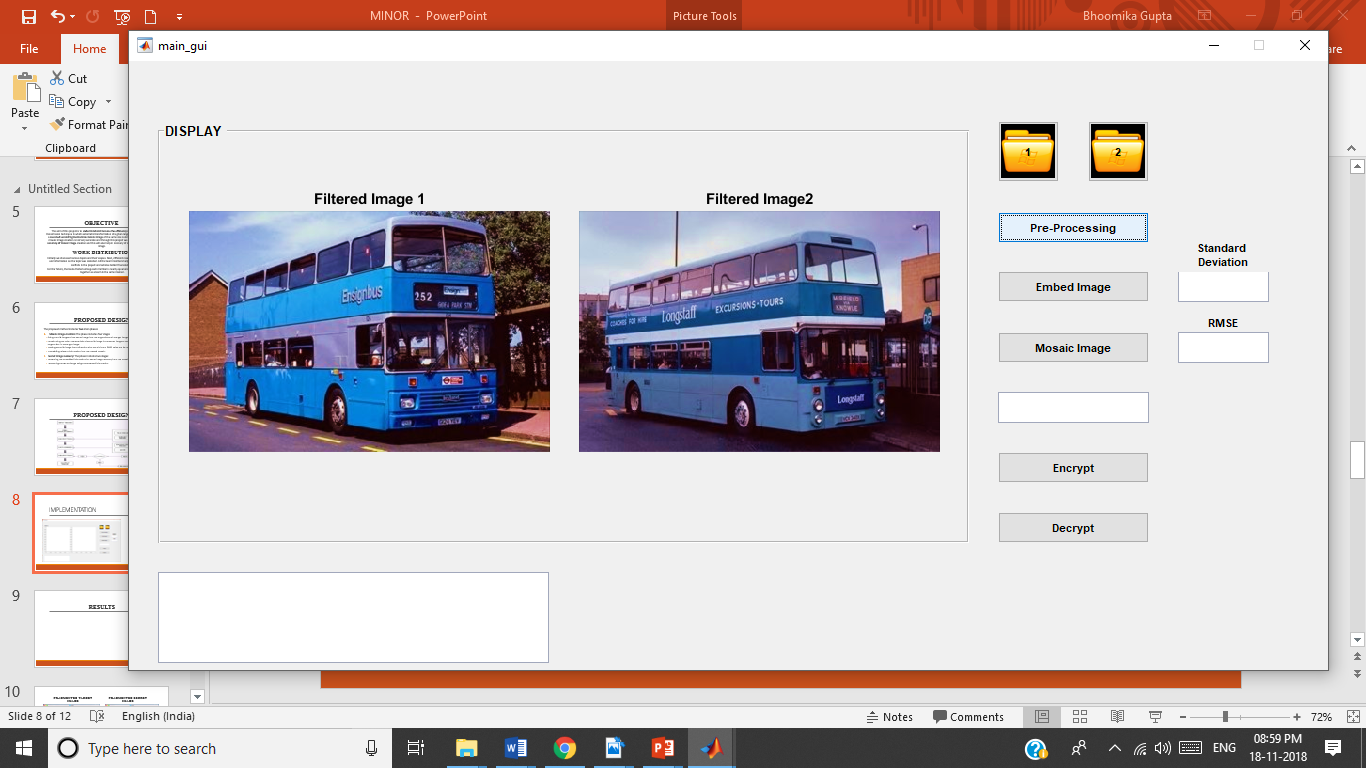
****

Figure 7: Pre- processing

* Embedding embeds the secret image into the target image.

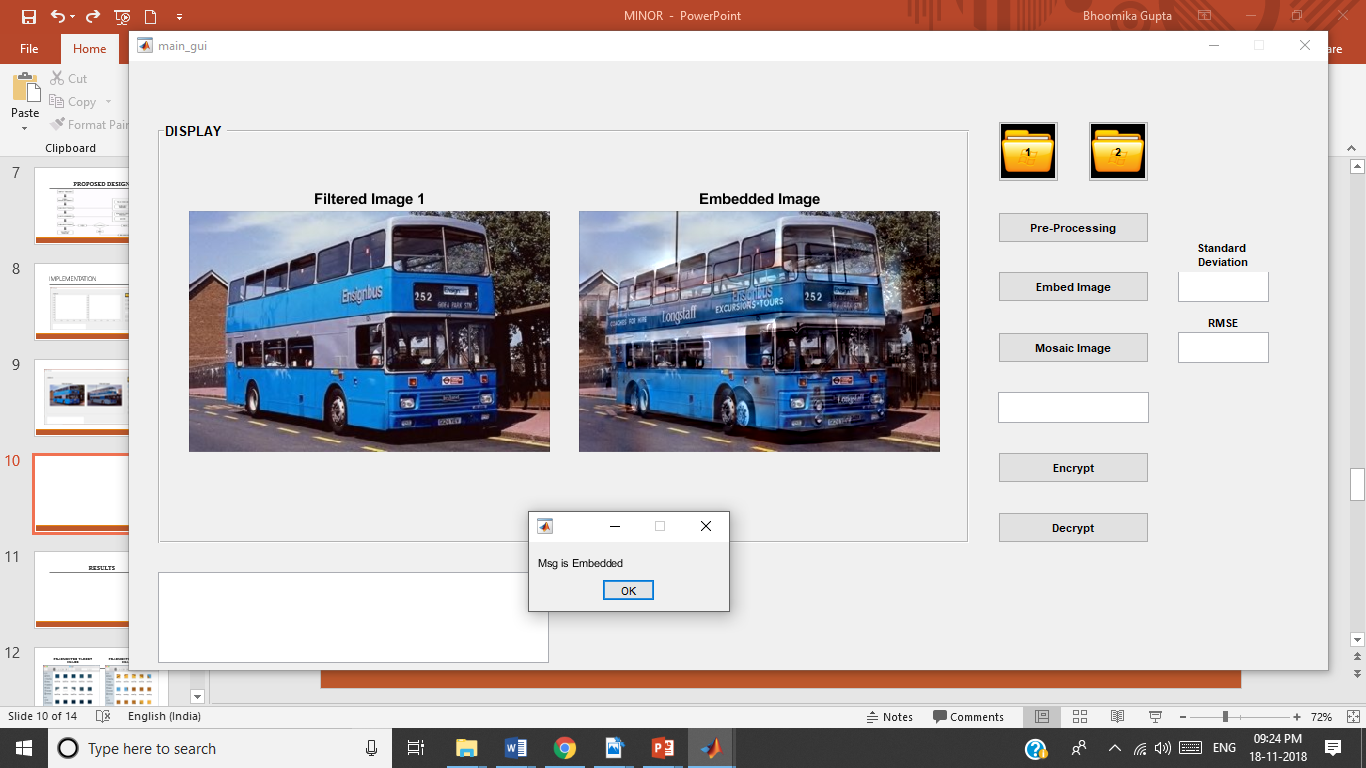


Figure 8: Embedding Process

* Mosaic Image creation creates the final mosaic image.

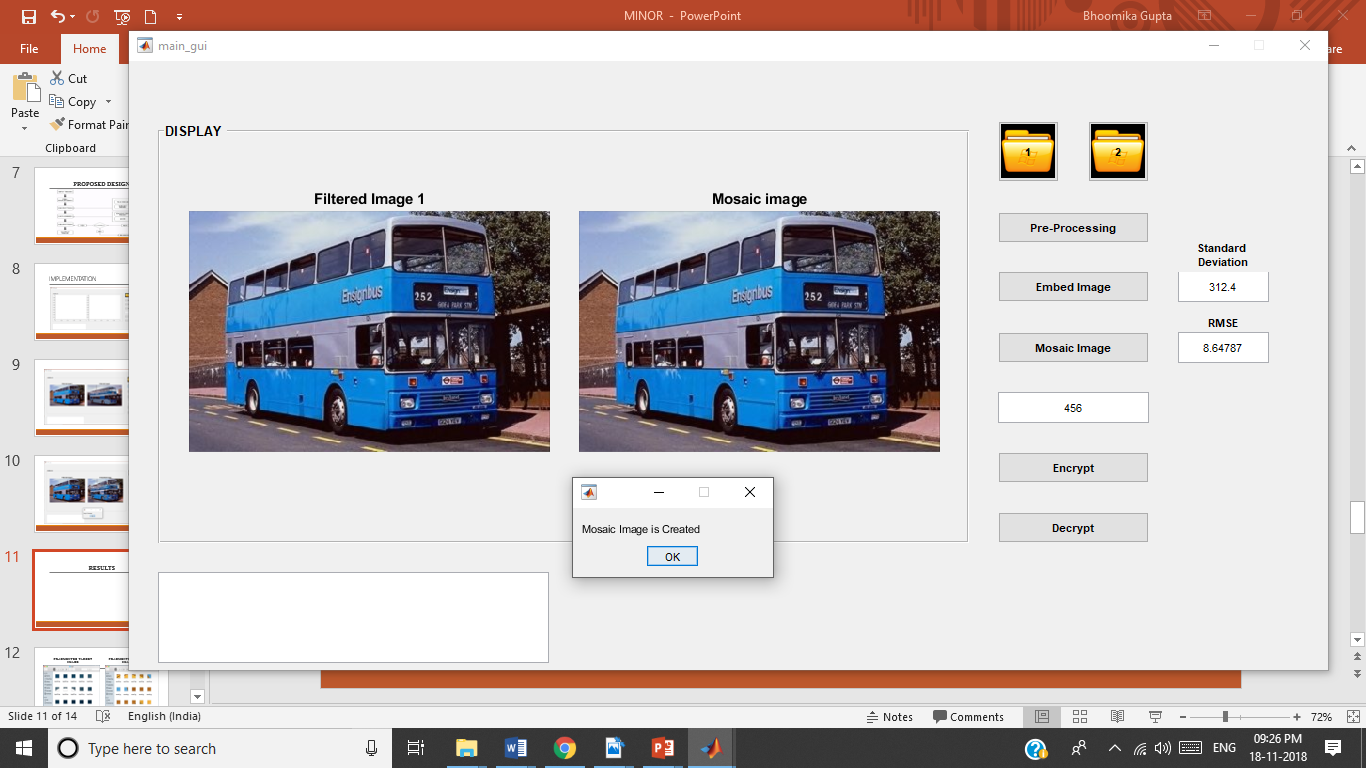
****

Figure 9: Mosaic Image

**6.2 Decryption**

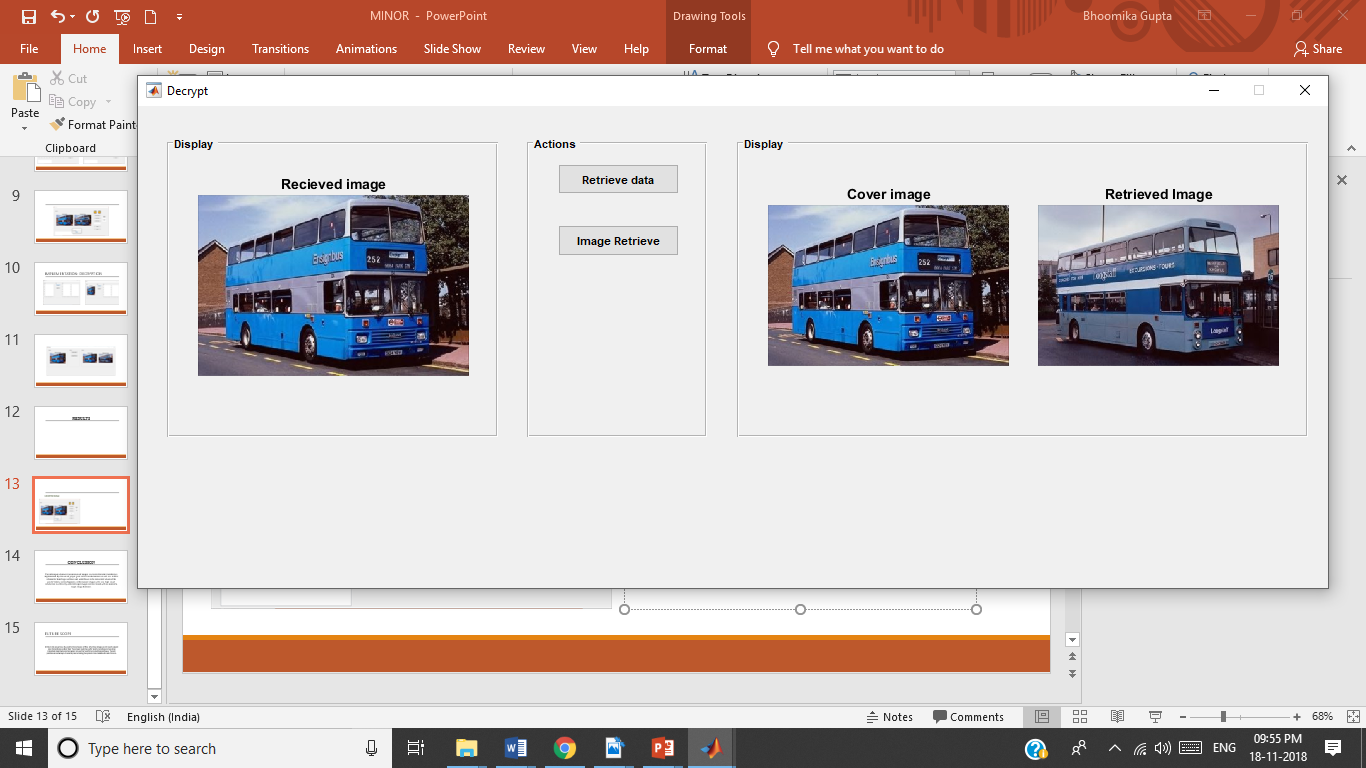
****

Figure 10: Decryption

**6.3 Limitations and drawbacks**

* Even though the images are resized, if there is a significant difference in their size and dimensions the image loses its properties while pre-processing and hence mosaic image creation is not possible.





Figure 12: Secret Image

* Figure 11: Target Image

Screen Shot 1940-08-29 at 10.36.06 PM.png

* According to the research proposed by Lee and Tsai, any arbitrary image can be chosen as the target image but the results have shown that the colour characteristics of the secret and the target image must be similar to get more secure mosaic image.

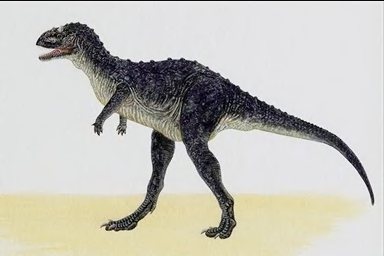
** **

Figure 14: Target Image

Figure 13: Secret Image

****

Figure 15: Resultant Mosaic Image

**CHAPTER 7: CONCLUSION AND FUTURE SCOPE**

The technique of secure transmission of images via reversible colour transform is implemented. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels’ colors, secret-fragment-visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Further, an attempt to increase efficiency and security is made.

In future the project can be used for transmission of files other than images and it could support color transmissions other RGB. The project could be useful tool for sending and receiving important data that could be hacked or used for harmful and unethical purposes. The key provides an extra layer of security hence making the system more reliable and safer for use.

**REFERENCES**

1. 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.
2. C. G. Soumi, J. George, and J. Stephen, "Genetic algorithm based mosaic image steganography for enhanced security," *International Journal on Signal and Image Processing*, vol. 5, no. 1, pp. 15-26, 2014.
3. 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.
4. 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.
5. Y.-L. Lee and W.-H. Tsai, “A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695–703, 2014.