Development & Analysis of Data Hiding Security Using Image Processing Technique.

Manjinder Kaur, Er. Sumit Chopra
[1]KC College of Engineering and Technology, Nawanshahr, Punjab, India.
(E-mail: sumitonhunt@gmail.com)
(E-mail: manjindergangarh@gmail.com)

Abstract— This paper incorporates a process we hide any text data and material in the image by using MATLAB programming. Stegano-graphy is the most common and useful techniques to hide any kind of data from robbery or unapproved individual. In spite of the extensive number of stegano-graphy transporters and strategies given by pictures, sound, and video are as yet the most widely recognized computerized bearers, and there is the gigantic number of stegano-graphy methods created.

Keywords— *Stegano-graphy, Data Hiding, Image Processing, Data security.*

I. INTRODUCTION

There are countless strategies through which instant messages is cover up with-in Advanced pictures (RGB, Dark scale and BW). The best way is abusing of useless parts of any documents or undefined memory for putting away mystery information which is likewise be straightforwardly gotten to. Small amount of data might be cover up with-in the free parts of the header documents [1]. In the event that segment isn't obvious in standard conditions, there are a few instruments which in the meantime permit full access. In spite of the fact that there are numerous stegano-graphy holders and the most prominent technique will be depicted in whatever remains of this paper. The fundamental standard of the framework dependent on the substitution is the substitution of excess parts of the picture with mystery information. For comprehension of this rule it is essential information of stegano-graphical holder structure, and we give a concise portrayal of the RGB (Red-Green-Blue) frameworks. With-in the RGB framework, each shading is spoken to by the general forces of every one of the three existing parts red, green & blue. Every RGB segment is dictated by a solitary octet, Since the RGB framework contains three segments, this technique for introduction, we get the 24-bit conspire which underpins 14,77,216 one of a kind hue. A large portion of the present applications for handling and showing pictures portrayed backings 24-bit conspire, yet permits the utilization of 8-bit plan to spare the picture measure. Such a plan entirely utilizes 24-bit shading pixels, yet furthermore has a palette that determines shading utilized in the picture. Pixels is coded with 8 bits, where is that esteem shown by the records wanted shading in the palette. Subsequently, this strategy confines the quantity of utilized hues in the picture at 256 for 8-bit. 8-bit design is run of the mill for GIF (Illustrations Exchange Arrangement) picture groups which are commonly viewed as a lossless picture pressure.

II. RELATED WORKS

A. Sorting Pallets

Countless pictures use shading palettes used in the image. Beds, clearly, contain only a subset of the entire shading space in 24-bit appear, and each shading in the palette is given a 24-bit vector that portrays the hued picture estimations of the shading record, ie the region of the bed. This rundown is secured with-in each pixel pictures and use it to choose the fitting shading pixels. The underlying stage in the execution of this stegano-graphical frameworks is making copies of the primary shading palette and change of territory in the new shading palette. The new shading arrangement is controlled by the tones that are close to the color structure, are in short proximity. By then applies a standard Lower significant bit substitution, that will at any rate criticalness with-in each pixel is superseded by bit riddle texts. Around the complete of the individual RGB shades perceived in the main bed, so its record in the primary group is used as the new estimation of the pixel.

B. Domain Transfer

The Change area in stegano-graphy procedure depends on concealing information utilizing scientific capacities. Numerical capacities are utilized in pressure calculations. The essential standard is to inclusion bits of mystery instant messages to put the minimum significance coefficients. In particular, the JPEG picture organize utilized discrete cosine change coding rather than individual pixels. Photograph split into 16x16 squares for every part of the Colored image framework. The objective is to discover hinders in which the measure of changes of the low pixels to the whole square is supplanted by a discrete cosine change coefficient. On the off chance that the measure of progress is excessively high, the square is isolated into 8x8 littler squares until the measure of the change isn't low enough [2]. JPG design is viewed as a picture pressure with misfortunes. The Image isn't exactly indistinguishable to its unique picture which is gotten with change. JPG stegano-graphy as carrier performed change the connection of these coefficients rather than bits in the LSB substitution.

C. Substitution of Important Bit

Substitution of least imperative bits is the most widely recognized stegano-graphy method utilized in stegano-graphy work with mixed media documents. The expression "least essential piece" is related with the numerical significance of the bits in the octet. The bit of greatest significance is with the most noteworthy number juggling esteem (12710), and the bit of least significance is with the least number-crunching esteem (120). Change of least bits has significance impact in all octets that make up a mixed media record. The depicted guideline is much progressively successful because of the way that the human optical arrangement isn't sufficiently touchy for Recognizing these adjustments in shading. The thought stegano-graphical procedures substitution bits' slightest significance depends on breaking the mystery instant messages on bits which are then kept set up for at any rate essential bits in chose octets. As a basic case of LSB substitution is demonstrated concealing the letter 'G' in the following arrangement of bytes:

10001101 00011101 110101111 10110100
00001111 11000001 100011011 110110110

The letter 'A' is the ASCII (American Standard Code for Information Interchange) standard recorded as a parallel string 0100011101. These 8 bits are kept in touch with the situation of the minimum vital bits in the first arrangement of bytes:

10001101 00011101 110101111 10110100
00001111 11000001 100011011 110110110

In the referenced model really changed just a large portion of the bits of the minimum significance. LSB substitution is stegano-graphical systems whose application is frequently not all that basic. Truth be told, if a lot of bytes into which is embedded through mystery instant messages will pick the easy way, for instance, a progression of contiguous bytes in the start of the document, all things considered, this piece of the pictures have diverse measurements from whatever remains of the picture, and in that capacity will attract regard for themselves and trade off the mystery of the shrouded instant messages. In this way, the set target octet frequently characterized by a technique for arbitrary choice as one of the elements that make discovery stegano instant messages greatly entangled. Pursued a case of concealing one picture to another, utilizing the given calculation.

III. ALGORITHM

The best strategy of advancing pixels. This technique changes the esteem estimation of an explicit number of pixels. Each pixel has its very own 3 octets, for every one of the 3 segments on the double. In case rather a part of the shading sections ASCII estimation of the characters in this pixel [4], the substance of the picture change, yet the human eye can't have challenged if using fitting picture. Sought after introduction of MATLAB limits that stow away and later scrutinizing the string from the image, as demonstrated by a key agreed. The basic flow chart of our work are as follow:
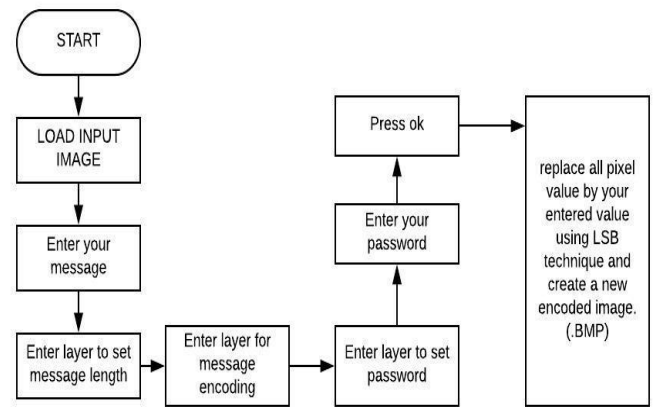

Figure1. (Flow chart encoding part)

In encoding part, firstly we have to load or browse the stegano image in which you want to embedded the data by using UIGETFILE function. Then enter your message which you want to embed. We know that RGB image have 3 layers (Red, Green and blue), so we embed our information in any layer. We enter 4 main values to hide the message i.e. Message layer, Length layer, password layer and Password. Password should ne the number and between 0-255 (unsigned integer range). Hit the ok pushbutton and by using LSB technique, pixels is be replaced by our data and then system recreate the new image i.e. Encoded image. The new created image is in BMP format. Because BMP is high level image.
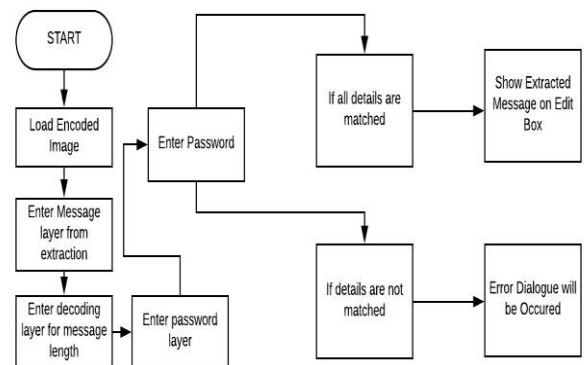

Figure2. (Flow chart decoding part)

Figure 2, represents the decoding part. Again we browse the encoded image in which we encoded the data. For extraction we have all information regarding message layer, length of message layer, password that is created by user and password length. If we have all info regarding the layers then only we have extract the data, otherwise an error dialogue will be occurred. And we unable to extract the original message from the encoded image.

Figure,3. (Normal Image)

```
global img
[File,Path] =
uigetfile({'*.jpg';'*.png';'*.gif';'*.bmp'},'Select
"IMAGE" to Hide Message.');
img = imread([Path,File]);
imshow(img);
```


Figure,4. (Encoded Image)

```
global img
global Message
global len
global Msglayer

global passlayer
global password


for i=1:len;
if Msglayer==1;
img(2,i,1)=Message(i);
elseif Msglayer==2;
img(2,i,2)=Message(i);
else
img(2,i,3)=Message(i);
end
```
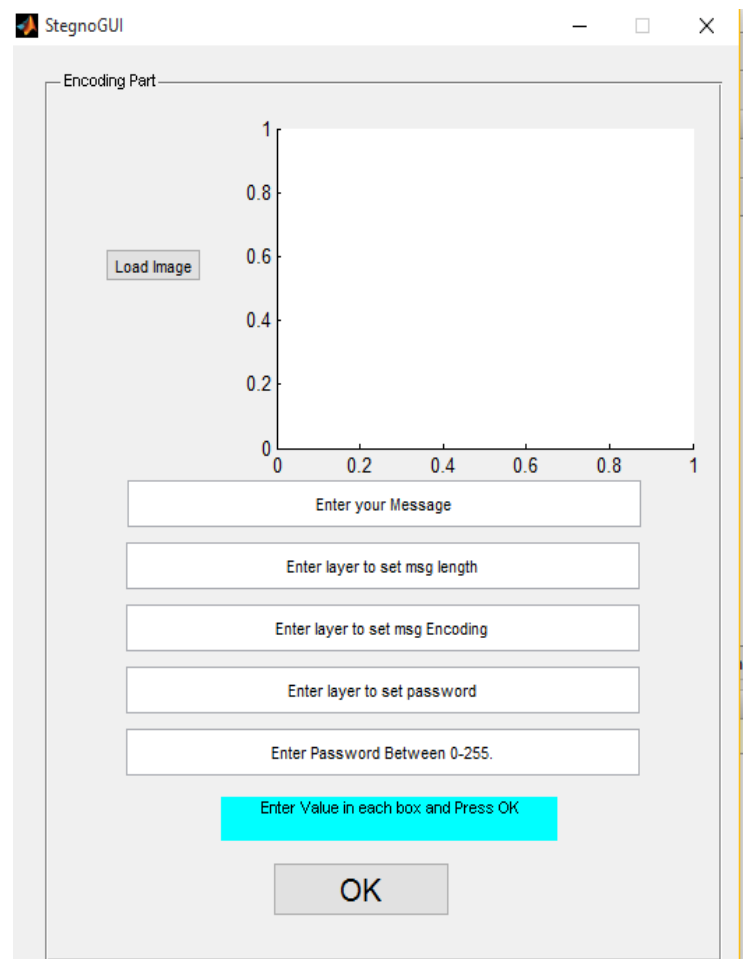
```
end
if passlayer==1;
img(3,1,1)=password;
elseif passlayer==2;
img(3,1,2)=password;
else
img(3,1,3)=password;
end

imwrite(img,'encoded_Image.png')
```

IV.   RESULTS AND DISCUSSION

Here is the proper GUI of our system. The project is based upon the image processing and interface with guide toolbox. That is easy to use. The systems look are as follows:

Fiugure,5. (Encoding part)

Figure 5, represents the encoding system interface. In algorithm the fig. 1 shows the complete working and flow chart of the encoding part. LSB technique is widely used technique in data hiding programs.
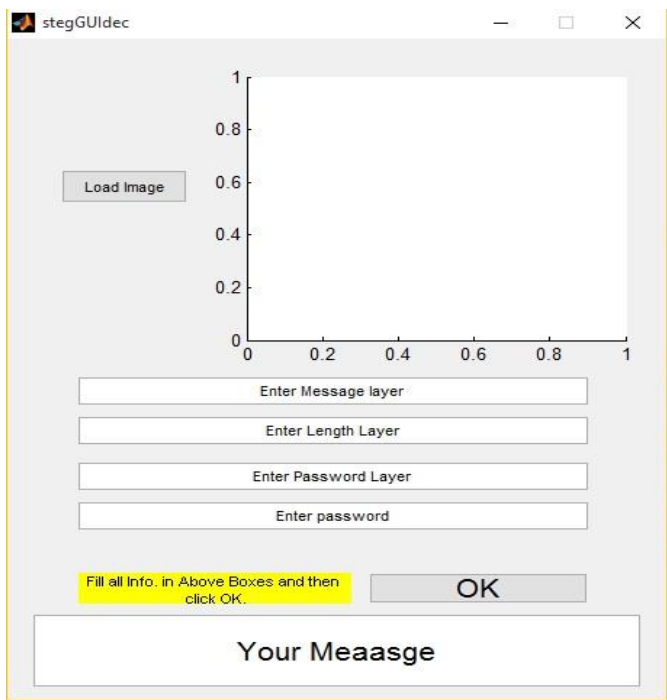
Figure,6. (Decoding part)

The decoding interface shows in fig. 6 and the algorithm of decoding part shows in figure 2. The extracted text will be shown on edit text (your message).

V.   CONCLUSION

Stegano-graphy is an exceedingly amazing systems that enable individuals to ensured and shroud correspondence. By using cryptography, will gives you an extrs security. Stegano-graphical innovation is exceptionally easy to utilize, and to a great degree hard to recognize. As of late, stegano-graphy is the subject of numerous talks identified with its maltreatment, particularly in psychological oppressor exercises.

In the previous years, stegano-graphy has been the subject of numerous discourses identified with its maltreatment, particularly in fear based oppressor exercises. So in numerous legitimate experts is developing worry about the utilization of stegano-graphy to share unlawful material by means of media records on sites. Steganalysis an a lot more youthful control of stegano-graphy. Today there are distinctive stegno techniques by which we effectively recognize and avoid such criminal exercises.

Then again, there are numerous points of interest of utilizing stegano-graphy in lawful setting, for example, advanced watermarking to decide responsibility for or more secure techniques for putting away critical and secret data, in this way, in future increasingly concentrated improvement of the innovation and the large number of applications conceivable outcomes. Matlab has huge open doors for graphical information, vectors and grids, and the documentation and print these charts. There are abnormal state capacities for 2-Dimensional and 3-Dimensional information perception, picture handling, liveliness.

REFERENCES

[1] Ahmed, A. M., & Day, D. D. (2004). Applications of the naturalness preserving transform to image watermarking and data hiding. *Digital Signal Processing, 14*(6), 531-549. doi: 10.1016/j.dsp.2004.08.002

[2] Alturki, F., & Mersereau, R. (2001, Apr 2001). *A novel approach for increasing security and data embedding capacity in images for data hiding applications.* Paper presented at the Information Technology: Coding and Computing, 2001. Proceedings. International Conference on.

[3] Amat, P., Puech, W., Druon, S., & Pedeboy, J. P. (2010). Lossless 3D stegano-graphy based on MST and connectivity modification. *Signal Processing: Image Communication,   25*(6),   400-412.   doi: 10.1016/j.image.2010.05.002

[4] Awwad, W. F., Mansour, R. F., & Mohammed, A. A. (2012). A robust method to detect hidden data from digital images. [Report]. *Journal of Information Security, 3*(2), 91+.

[5] Babu, K. S., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. (2008, 19-21 Nov. 2008). *Authentication of secret information in image Stegano-graphy.* Paper presented at the TENCON 2008 - 2008 IEEE Region 10 Conference.

[6] Chandra, M., & Pandey, S. (2010, 1-3 Aug. 2010). *A DWT domain visible watermarking techniques for digital images.* Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On.

[7] Chang, C.-C., Chen, W.-J., & Le, T. H. N. (2010). High payload stegano-graphy mechanism using hybrid edge detector. [Report]. *Expert Systems with Applications, 37*(4), 3292+.

[8] Chen, W.-Y. (2007). Color image stegano-graphy scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. *Applied Mathematics and Computation, 185*(1), 432-448. doi: 10.1016/j.amc.2006.07.041

Manjinder Kaur is persuing M.tech from KC College of Engineering & Technology, Nawashahr. The area of field is Computer Science. Her research work includes image processing   and   data   security.