(IJIEST) 2021, Vol. No. 7, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

Developing an Alternate Steganography Approach for Enhancing the Security Safeguards in Multilayers of The PNG Images

Aarushi Chawla

ABSTRACT

Steganography hides important information in a masked structure to hide the Presence of individual information and the original condition. This paper proposes another Steganography strategy, which utilizes different layers to conceal the information. The system proposed is a PNG picture-based method. Unlike additional information hiding Methods in which BMP or gif images design is used, this technique uses PNG pictures in which the innovation of the RGB layer is profoundly saved even in the wake of Stagnating the Image. In this multi-facet approach, we Proposed a way for the two texts to image and image to image Steganography. In this technique, The plain text is encoded into the cover picture, and the resultant image is acquired with plain text embedded. The resulting drawing is additionally encoded inside another cover picture as a second coming about the image, with an image placed in it; by this methodology the how close to base information is put away, and the type of its reality is profoundly inconsistent, it is exceptionally Robust from Attacks even a positive attack can't deliver the specific consequences of privileged information as the information is put away in various structures in various layers. Thus, security is profoundly upgraded in this proposed strategy, and the hiding limit is exceptionally Improved.

I. INTRODUCTION

Security is the main concern in today's modern world, to hide a sensitive piece of data from intruders and hackers became a difficult task. In cryptography we use certain Techniques to encode the data using a key and the encoded secret data is Decoded using the same key or different key shared by the sender to decode. In cryptography one can predict message is encoded but cannot decode without key. But in Steganography one cannot predict the data is encoded or its form of existance.In Steganography we encode the message inside a media and the original form of secret data is changed, so the secret data is hidden and its form is unknown to predict. Steganography can be involved in two categories: 1.Linguistic Steganography, 2.Technical Steganography. Here our interest is the technical Steganography Technical Steganography is further classified as follows 1.Text, 2. Image, 3. Audio, 4.Video, 5. Protocol. The data hiding is possible in the above formats because of the existence of high redundancy bits in the above digital media. Higher the redundancy bits higher the possibility of manipulation .In text Steganography the plain text is hidden in the image or in the video file In image Steganography the image is stored inside other image or in a video file .In audio Steganography the audio file is hidden inside another audio file or other media file. In video Steganography the video is usually hidden inside another video file. or a still image can some image files that are combined to form a video file.In protocol Steganography the network protocols are hidden for secret communication. Though each of them has their own importance The Image Steganography is widely used because of its wide possibilities in manipulating the pixels. Many data hiding methods are proposed recently but this proposed method has some unique features to hide the data. Here in our Article we discuss a method for both Text-Image and Image-Image Steganography. In this case a text message is hidden it in the image concealing the existence of its form as text data so that the intruder cannot guess there is an existence of secret data in the form of text encoded inside the image which further encoded inside other cover image. The above method we are going to propose

is an image Steganography method, In this new method we use a multi layer of security.This lets the method robust from Steganalysis which is detection of the existence of Steganography in the given digital media.

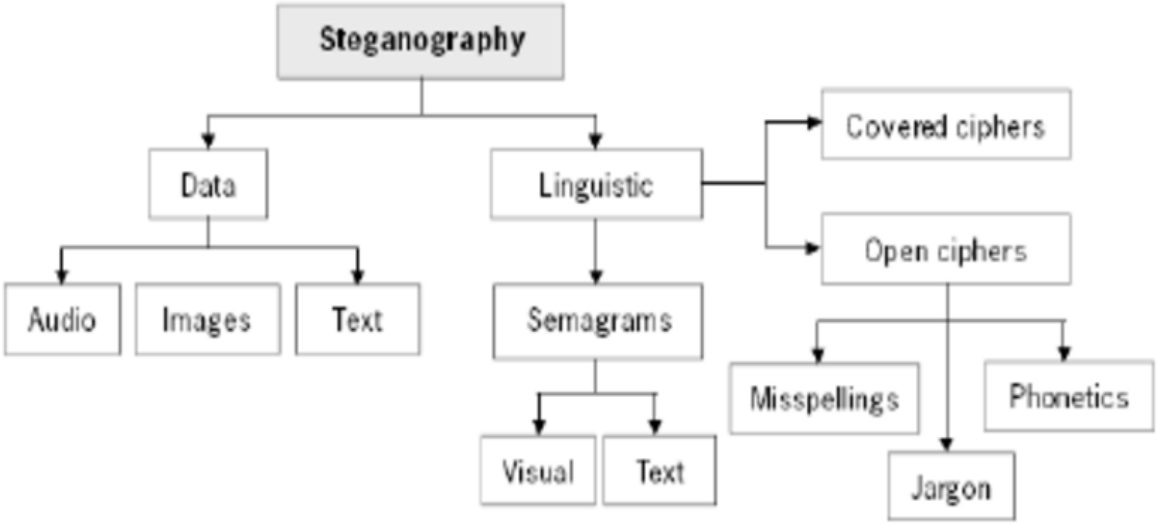

Fig 1: Steganography Classification

II. ESSENTIAL TERMINOLOGY

Cover picture: A cover picture is a picture the information is normally concealed inside

Individual information or payload: Secret data is the information to be covered up. It very well may be in text, a thought, a video document, or a sound record.

Steganography calculation:

- There are numerous strategies in Steganography.
- The analysis is chosen dependent on the limit and type of individual information and security issues.
- LSB (LEAST SIGNIFICANT BIT) is perhaps the most usually utilized technique.

Steganoimage or Stegogramme: SteganotImaimage is the resultant Image gotten in the wake of encoding the restricted information in the cover picture utilizing the Steganography calculation.

(IJIEST) 2021, Vol. No. 7, Jan-Dec e-ISSN: 2454-9584; p-ISSN: 2454-8111

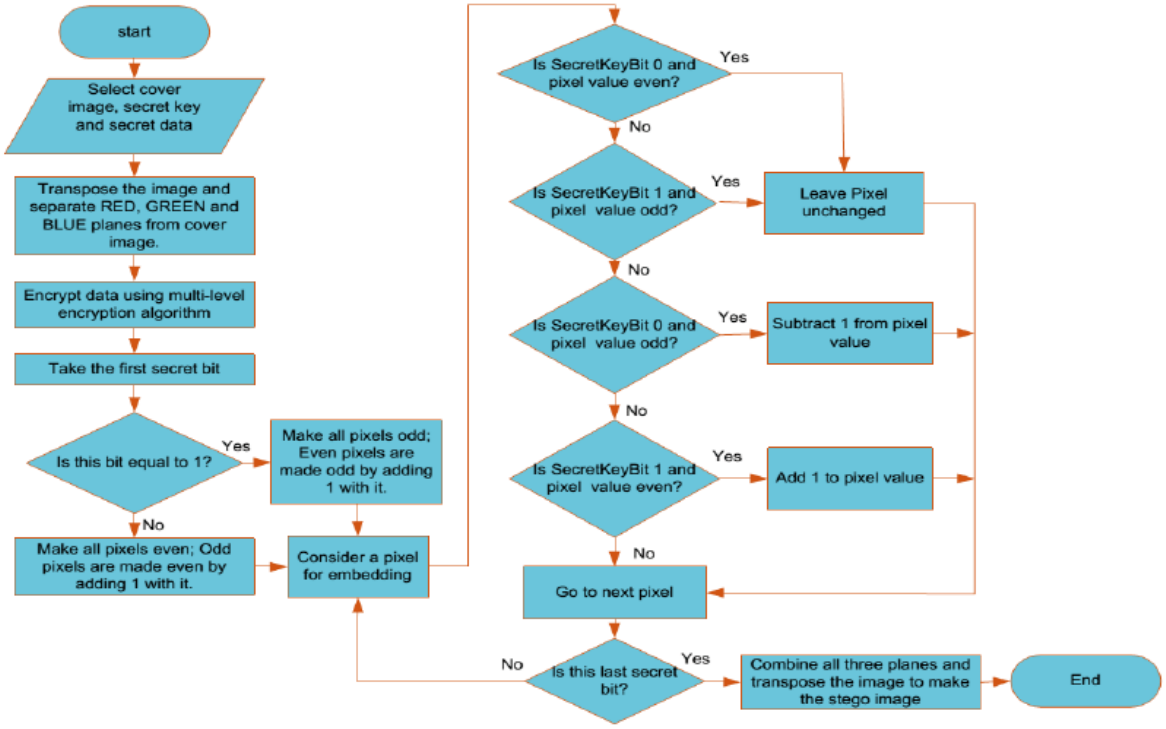

Fig 2: Embedding process flowchart

III. RELATED WORK

Steganography is applied to both the change space and spatial area. In the changing room, the broadly utilized techniques are JSTEG (JPEG Steganography), DWT, etc. In the spatial field, the LEAST SIGNIFICANT BIT (LSB) strategy is generally used.

3.1 LSB (Least Significant Bit) METHOD

LSB in BMP, LSB in gif, LSB in PNG is generally utilized. In the Simple LSB method for RGB shading pictures, every pixel shading part is separated into 8bit paired strings in the ASCII design. The most un-huge piece is altered on the chosen shading to conceal the information string.

Model: Let "s conceal an information String utilizing the LSB technique; 01111010 is the string to stow away into an 8-cycle shading picture. What might be compared to those pixels possibly like this:

01101100 10101111 11011010

Fundamental MODEL OF STEGANOGRAPHY

The essential model portrays how the information is inserted and separated.

The double string 01111010 is supplanted in each LSB bit from left to right to in the pixel values Image picture; the returned bit example would be

01101100 10101111 11011011
01101011 10101101 10111010
10011011 10111000

The paired string 01111010 (decimal worth 122) is subtly concealed inside the LSB "S of the pixels.

Yet, This Technique is not difficult to recognize, and pornography to attack, so this new strategy is proposed to address this issue.

(IJIEST) 2021, Vol. No. 7, Jan-Dec e-ISSN: 2454-9584; p-ISSN: 2454-8111

IV. THE MAIN GOAL OF THE STEGANOGRAPHY TECHNIQUES ARE [1,2]

1. Huge information concealing limit

2. High security

3. Higher PSNR esteems

V. PROPOSED METHOD

In this strategy, the mysterious message encoded is changed to a surge of 6-digit paired information per character. This parallel information is encoded into the blue shading part of pictures picture) consequently framed has the mysterious message encoded into pictures is additionally encoded into another photograph). Every pixel of an Image picture requires three pixels of the imaged picture for inserting their qualities into them. The red worth of the pixel of pictures picture is encoded into the RGB upsides of the pixel of the reflected view.

```
1: function WMB(step)
2:     c ← ReadCoverImage()
3:     msg ← GetRandMessage()
4:     ACw ← ACCoefWatsonModel(c, step)
5:     for each AC coefficient i
6:         Xwlh_i ← LowPrecHist(ACw_i, step)
7:         (p_i, s_i) ← FitGCD(Xwlh_i, step)
8:         cdf_i ← ComputeCDF(p_i, s_i)
9:         symP_i ← SymbolProbability(cdf_i)
10:    end for
11:    order ← RandPermutation()
12:    newSym ← ArithEncode(msg, symP, order)
13:    newXw ← NewCoefficients(newSym)
14:    s ← WriteStegoImage(newXw)
15: end function
```

Fig 3: Encoding pseudocode

(IJIEST) 2021, Vol. No. 7, Jan-Dec e-ISSN: 2454-9584; p-ISSN: 2454-8111

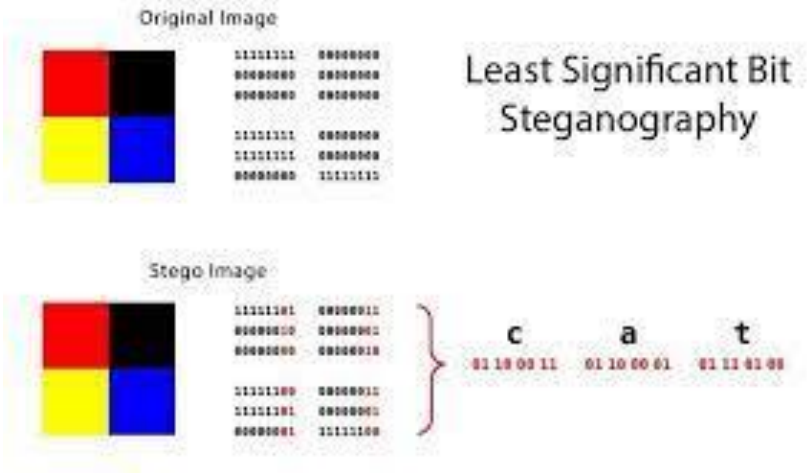

Fig 4: Pixel Modification after encoding

Likewise, the green and blue upsides of the pixel of pictures picture are installed into the following two successive pixels of the imaged picture. During extraction, the thought is first extricated. This extracted Image has secret text encoded into pictures. The interpreting calculation additionally handles painting to eliminate the individual reader.

VI. TEST RESULTS

The outcomes in this configuration are determined utilizing the PEAK-TO-SIGNAL-RATIO(PSNR). The PSNR estimates the coordinating of the picture with the Stegnographed Image by assessing the highest conceivable force sign of the picture with the imaged picture. Here for our situation, the picture is the cover picture, and the picture is the arranged picture. Higher the PSNR better the outcomes filed in this specific situation, we classified the correlation of PSNR of different strategies with the proposed method. The proposed calculation was carried out in MATLAB (R2015 a) running on Windows 10 Operating System. The pictures utilized are 265x265 standard PNG Format pictures, in particular Lena, Baboon, Pepper, Boat and the tried message limit, and the Method names are classified to analyse.

Table 1. PSNR value comparison of 3-Methods and suggested method

Cover images	Message capacity	PSNR			
		DWT	Method [4]	Parity checker	proposed method
Lena	1000	60.3033	63.0432	65.0202	66.2011
Babbon	1000	60.2393	63.0220	65.0789	66.3276
Pepper	1000	60.1	63.0535	65.0440	66.2567

Table 2. PSNR value comparison of 4 different Methods and proposed method

Cover images	Message capacity	PSNR			
		SLDIP	MSLDIP	Method [5]	proposed method
Lena	6656	44.9886	48.7596	48.823719	58.0829
Boat	6656	44.9953	48.6661	48.894425	58.1030
Babbon	6656	44.9953	48.6638	48.684503	58.0530

VII. CONCLUSION

In this article, another Steganography strategy is Proposed for multi-facet information stowing away; The proposed technique has high PSNR Values contrasted, and a Few Existing Methods like SLDIP[1](substitute last digit in pixel), MSLDIP[1] (Modified substitute last digit in pixel), JPEG-JSTEG[7], Parity Method[6], DWT[8], the outcomes are classified. Our primary point in this article is to get the information, safeguard the picture quality, and increment information concealing limit. The above-proposed strategy doesn't eradicate the originality Image the picture; utilizing this new multi-facet approach, information security is profoundly improved; the high PSNR esteems are gotten because RGB layers Image the picture is used safeguarded well; however, a few techniques have comparative PSNR admires. In any case, this technique is profoundly suggestible as security is the real worry in this field. Further investigations propose applying this strategy for video information stowing away and a couple of Security Enhancements.

REFERENCES

[1]. Radwan, A. A., & Swilem, A. seddik AH,"A high capacity SLDIP (substitute last digit in pixel) method.In fifth international conference on intelligent computing and information systems (ICICIS 2011) (Vol. 30).

[2]. Deepa S., Umarani R., "A Study on Digital Image Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3,Issue 1, January 2013.

[3]. Abdelmgeid A. A., Al - Hussien S. S., " New Text Steganography Technique by using Mixed-Case Font ", International Journal of Computer Applications, Vol 62, No.3, January 2013

[4]. Marwa M. E., Abdelmgeid A. A., Fatma A. O. "A Modified Image Steganography Method based on LSB Technique." International Journal of

Computer Applications,Vol. 125, No. 5, September 2015.

[5]. Abdelmgeid A. A., Al – Hussien S. S., " New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM) ", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 2, Jun 2013.

[6]. Tahir A. and Amit D.” A Novel Approach of LSB Based Steganography Using Parity Checker” International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 1, January 2015.

[7]. S. K. Muttoo , Sushil K. "Data Hiding In JPEG Images", BVICAM'S International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi, Vol. 1, No. 1 January – June, 2009

[8]. Arun R. , Nitin S. , Eep K. "Image steganography method based on kohonen neural network." International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012.