Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

A novel steganography technique using grayscale image segmentation

Fakhar Ullah Mangla [1,*], Saira Nokhaiz [2], Muhammad Ramzan [1], Ikram Ullah Lali [3]

[1]*Department of CS and IT, University of Sargodha, Sargodha, Pakistan*
[2]*Department of Computer Science, University of Lahore, Lahore, Pakistan*
[3]*Department of CS and IT, University of Gujrat, Gujrat, Pakistan*

ARTICLE INFO

Article history:
Received 25 October 2018
Received in revised form
21 February 2019
Accepted 25 March 2019

Keywords:
Steganography
Cover image
Secret message
Least significant bit substitution

ABSTRACT

Steganography is used for invisible secured communication. In this technique, information is hidden on different medium like audio, video, text, or images by using different approaches or algorithms. This research has developed a novel steganography technique which combines grayscale image segmentation and least significant bit (LSB) substitution methods to hide information. In the proposed technique the cover image is segmented in a different number of blocks. Each block hides just one bit of information in its LSB. The number of blocks is directly proportional to the size of the information in bits. In such a way, information is hidden in the whole image, not in a specific area of an image, so there is no image degradation.

1. Introduction

Steganography is the composition of two Greek words 'Steganos' mean covered, and 'Graptos' mean writing. According to Pftizmann (1996), this cover writing technique is used for invisible communication. In steganography, the information which we want to transmit secretly to the destination is concealed in another type of medium like an audio file, video file, or an image file. This approach is systematic, its primary purpose is not only to hide the message, but it also hides the existence of the message or conversation. According to Avcibas et al. (2003) there are four characteristics of steganography that should exist in steganography to make it great approach whese are as follows: Undetectability, Invisibility, security, payload capacity, and robustness (Avcibas et al., 2003).

1.1. Steganography vs cryptography

Steganography and cryptography are entirely different concepts, and these techniques work differently to protect data. Steganography protects information by hiding the appearance of conversation. So it is impossible to detect the existence of the message this thing makes it more secure because when conversation is hidden nobody try to read it while cryptography protects information by encoding it in another form which is not understandable, so nobody can read it because this encoding is done by using some mathematical formula. Table 1 shows the comparison of steganography vs, cryptography.

Table 1: The comparison of steganography vs, cryptography

Steganography	Cryptography
The existence of communication is hidden.	The existence of communication is visible in cryptography.
Encryption is not necessary because the existence of the message is unknown	Encryption is used to change the actual message to prevent it from an unauthorized person.
Steganography does not change the secret message before transmission.	Cryptography changes the message before sending.

There are following types of steganography according to a medium that is used to hide data: Text, Audio, Video, and Image. Changder et al (2009) have presented a novel approach for Indian text steganography. In this technique, perceivable sentences are formed to hide the obscure message. In this approach, strings find to make a sentence by using the longest ordinary subsequence. It is revealed that text steganography is difficult in all types of steganography due to deficiency of duplication of text and zero overhead (Manjula and Danti, 2015).

XOR is performed on the LSB and next to it. If the secret message bit is 0 then result of XOR is 1, and if the bit is 1, then the result will be 0. We can retrieve the message by XORing the LSB and 2LSB. After retrieving every 16 bit, it is converted to the

[*] Corresponding Author.
Email Address: fmangla@yahoo.com (F. U. Mangla)

https://doi.org/10.21833/ijaas.2019.05.014
Corresponding author's ORCID profile:
https://orcid.org/0000-0003-2116-9959
2313-626X/© 2019 The Authors. Published by IASE.

corresponding decimal value (Balgurgi and Jagtap, 2012).

PPM stands for Pixel Pair Matching that uses two pixels to hide digits in the binary notational system. APPM stands for Adaptive Pixel Pairing Matching allow concealing digits in any notational system. This approach uses two pixels one for reference coordinate, and another is used for search coordinate (Rosaline and Raj, 2013).

1.2. Hierarchy of steganography domain

There are two domains of steganography; spatial and Transform. Both domains are categorized in many types, which are represented in the Fig. 1.

Table 2 describes the advantages of different transform domain technique proposed by different authors.

Table 2: Comparison of different transform domain techniques

Author	Method Used	Advantage
Tiwari et al. (2014)	LSB Based Steganography Method	High Capacity and good MSE and PSNR
Sravanthi et al. (2012)	Plan Bit Substitution Method	Sufficient To discriminate analysis of stego and cover image
Viswanatham and Manikonda (2010)	LSB Insertion Mechanism, Random Number Generation Algorithm	Secure transformation of data
Alam et al. (2011)	Noise filtering before embedding combined with encryption	Error detection and noise free transformation

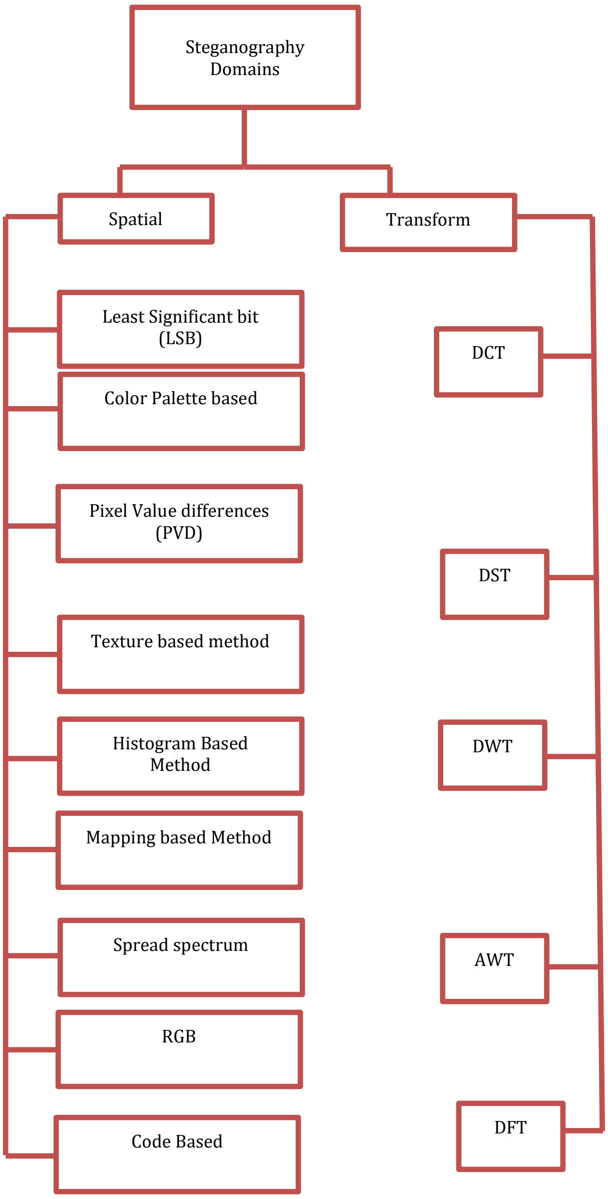


Fig. 1: Steganography domains

2. Literature review

Steganography and the cryptography are entirely different approaches. They have different strategies to communicate secretly. In steganography existence of the message is hidden but in cryptography message is visible, but it is not in a form that is understandable. But when these techniques are used collectively, it makes the secret communication more secure, reliable and robust. Firstly, encrypt the message than hiding in cover object make it more secure if anyone become able to retrieve a message that he would not be able to understand it due to encryption (Nilizadeh and Nilchi, 2013).

Steganography is a type of communication where the presence of the message is hidden in image, audio, video or text data but the most common and secure medium is an image that is usually used. This approach is advantageous due to sight power of human being to recognize variations in color that is limited. In image steganography both types of pictures can be taken, grey scale image or colored. Greyscale is best because of its less variation in colors due to the existence of just black or grey. In greyscale image color, variations are slight, so nobody easily judged it by the naked eye as a colored image when a large amount of data is hidden inside it. In image steganography, there are numbers of techniques, but LSB (the least significant bit) is the most commonly used technique (Hussain and Hussain, 2013).

To conceal data in the image by using the blind algorithm is the easiest way due to the manner in which it works. It just starts reading the pixel values of an image from the left top corner to the onward pixel by the pixel and hides information bit in each LSB of the pixel. The same procedure of image reading is used to decode information by changing the pixel values. This technique is not safe because the unauthorized person easily detects the existence of the message in it. When information that we want to conceal is finished than a remaining pixel of the image is unchanged, and image degradation occurs on the top area of the image where information is hidden, and rest of the image remains fine (Umamaheswari et al., 2010).

An array is formed by aligning the bits in a place. A cover image has selected that matches your choice, Secret message bit stream is placed over the resemble block from cover image that's why there is less image distortion (Zhang and Tang, 2007). In this improved steganography approach set of the pixel from the cover image is randomly selected. Pseudorandom numbers make this random selection each pixel embeds secret data bit by using the addition and modular division operator (Juneja and Sandhu, 2009).

The Gray Scale Image Steganography is the focus of this research. It is a robust and secure technique which is based on image segmentation and LSB (the least significant bit). In this technique, the images are converted into a 24 bitmaps virtual grayscale image, and then identified all the possible segments inside a picture, and then computed the potential areas for each segment with boundaries.

This knowledge is represented by the key of image segmentation, data distribution inside segment (area selection), the key of mapping within each area segment, key agreement of cryptography method, the key of secret message length and the key of message extension (Bawaneh and Obeidat, 2016). In this approach, a password is used to create a random seed that is used to take the first position where secret information bit is hiding. This procedure continues until the whole information is hidden. This approach is right in the sense of security because nobody can crack the algorithm, without knowing the password because we have to try each combination of the pixel in every order. This approach is also not the best approach because during hiding information it is not bothering the pixel. A pixel which is going to be changed and degrade the quality of the image may be useful. Maybe another area is better to hide data that we are not taking because of a random selection of the pixel. A tool of steganography uses this approach called 'Windows 95.' This tool also uses a password to create seed to choose the pixel for embedding the secret information in it (Vishal, 1992).

For increasing the capacity to hide data in color image, a technique is used to combine the characteristics of RGB intensities with a Triple-A algorithm that depend on randomization. This approach is applied to the color image where each pixel consists of three basic channels or colors red, green, and blue. Storage depends on the real pixel color values if it contains lower values than it would enable to hide large numbers of data bits. To store data bits, this algorithm uses the real color of the channel with the pseudorandom generator. This technique works well and gives effective results. Steganography becomes robust and secure when it is used with encryption (Rahman et al., 2016). When the encryption technique RC 6 is used with steganography, it gives an improvement in security. It also becomes a better approach when hybrid encryption techniques are used (Shrivastava and Singh, 2016).

There are a lot of steganography techniques for hidden communication. One of them is "pixel values difference" PVD module approach. This approach is used to get the best quality stego image than other methods. But there was a big drawback that comes in the notice is its low capacity to hide data than other techniques like LSB. This approach has the low ability because of the division of the pixel in smooth and edge blocks. In edge block pixel value, the difference is high while in the smooth block it is slow. To resolve this issue, Gadiparthi et al. (2011) proposed a new approach that is the composition of two approaches PVD and LSB that increases the hiding capacity experimentally.

In this approach, we keenly concern on the use of LSB technique for the smooth area of image and PVD module technique for the edge area pixel pair. To know in which are pixel pair is lying, we use threshold value. Suppose pixel value difference is 4 and the corresponding width range is 8 only 4 bit embeds while in LSB double data can be hidden we can embed 8 bits as well. So, to overcome this drawback both techniques are used at a time. To embed data two steps are used. In first step data is converted in binary and find the pixel value difference 'd'. In next step compare this value to threshold value, if it is less than the threshold value, it indicated that these pixels lie in smooth are than LSB technique is used otherwise PVD module comes in working (Gadiparthi et al., 2011).

3. Proposed technique

In this proposed technique segments are equal to the number of bits of secret information. Nobody knows the actual size of information in bits that is to be hiding. This approach is more secure and robust. Each bit of secret message is hidden in the LSB of each segment of the cover image. Proposed technique research framework is as Fig. 2.

Following is the example that briefly describes this proposed technique:

Example: "We are Muslims. We love our religion and our prophet" This is a secret message that we want to hide in a cover image of size 256*256. This message is converted in binary by the following formulas.

$$M = L \times 8 \tag{1}$$

$$S = {}^{N}\!/_{M} \tag{2}$$

where M = secret message size, L = letters of information, Eq. 1 tells the size of secret message size in bits, because 1 byte is equal to '8' bits that's why no of letters are multiplied by 8.

Eq. 2 is for the size of each segment in bits, where N is cover image size in bits and M is the Secret message size in bits.

Cover image size is 256×256. To convert it into bits, we multiply it by 8. Size of cover image in bits is $N = 256 \times 256 \times 8 = 524288$. Numbers of letters are 54 after calculations the received message size is 432. Size of the segment is $S = {}^{N}/_{M} = {}^{524288}/_{432} = 1213$.

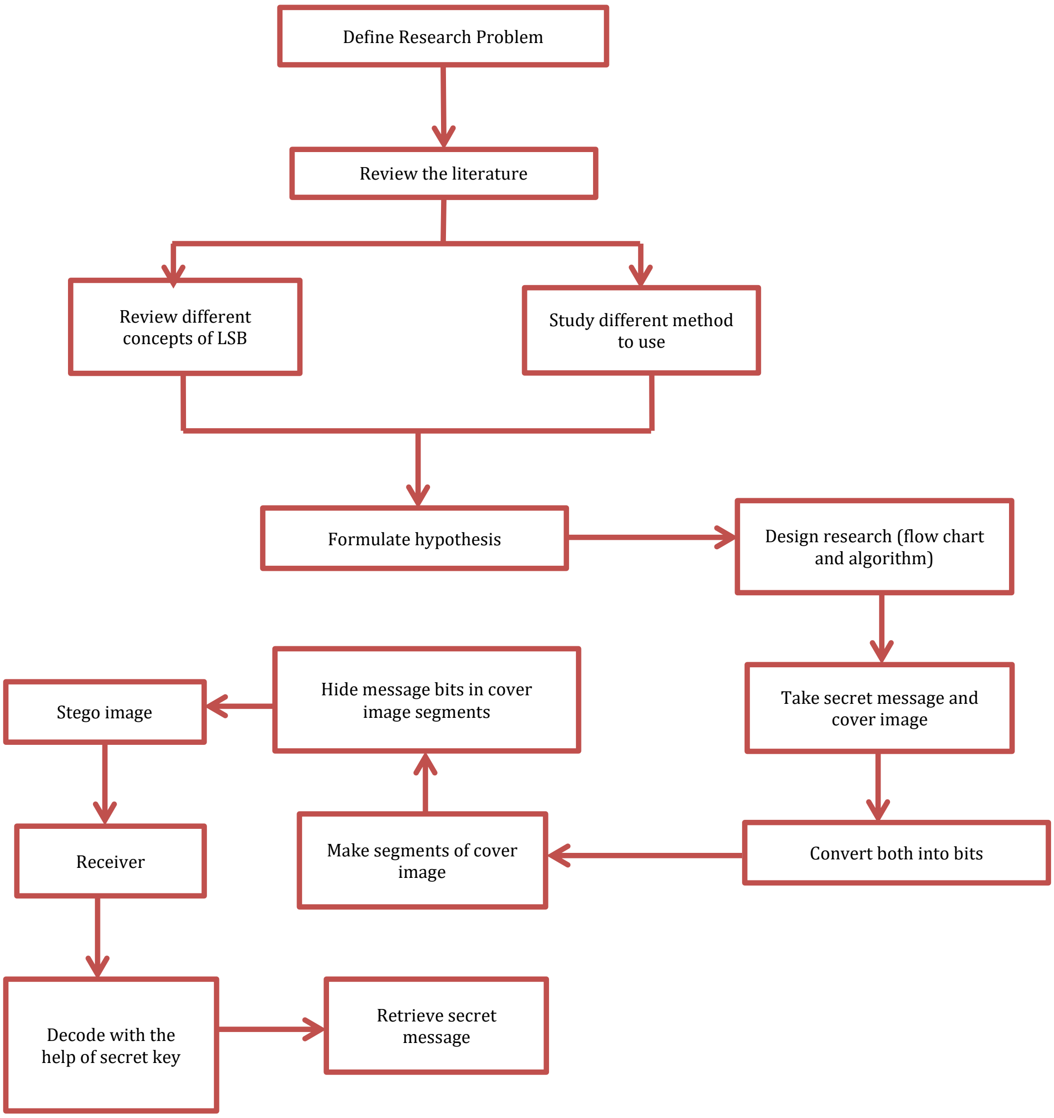

Define Research Problem
Review the literature
Review different concepts of LSB
Study different method to use
Formulate hypothesis
Design research (flow chart and algorithm)
Take secret message and cover image
Convert both into bits
Make segments of cover image
Hide message bits in cover image segments
Stego image
Receiver
Decode with the help of secret key
Retrieve secret message

Fig. 2: Research framework of methodology

Its mean number of segments is equal to the amount of information in bits. That is 432. Size of each segment would be 1213 bits so secret information bit is saved in 1213-bit next info bit is saved in the 2426th bit and so on, let explain this example step by step. In first step selected image is transformed to grey scale image if it is a colored image.

Step 1: Conversion from colored to grey scale image
Step 2: Image in pixel form that has decimal values
Step 3: Convert the Cover Image from decimal to binary.
Step 4: Convert the secret message into binary.
Secret message: 'We are Muslims, we love our religion and our prophet.'
Step 5: find the size of image and classified information in bits.

Let's take:

$N = r \times c \times 8$ //1 byte=8bits
$N = 256 \times 256 \times 8$
$N = 524288\ bits$
$M = L \times 8$
$M = 54 \times 8$
$M = 432\ bits$

It means the size of each segment is 1213 bits that are equal to 151 bytes. Numbers of segments are equal to the number of bits of secret message that is 432.

3.1. Encoding message in cover image

To encode the message in cover, image the following algorithm is used.

Information_encoded_Algorithm(N,n,s,msg,img

```
1. Hide[N] ← msg
2. K ← 1
3. Repeat step 4 while N= = n.
4. Repeat step 5 for i ← 1 to r
5. Repeat step 6 for j ← 1 to c
```

```
6.  Count ←count+1
7.  If count = = s
7.1 Img[I,j] ←hide[K]
7.2 K ←K+1
8.  Return
```

3.2. Working of information encoding algorithm

Initially, an array is declared to store the information bit if the size of the secret message in bits (N) is equal to the number of segments. Then a loop 'i' works from 1 to row and 'j' loop works from 1 to column, place each iteration in count variable until the count is equal to segment size(S). When it reaches its size, it stores the 1 bit of secret message (M) in LSB of that last byte of the segment.

In Table 3, the first segment is from 1 to 151 bytes and in last bit of last byte secret message bit is hidden. The segment is a block that is composed of multiple pixels or multiple bytes. Secret information bit always encodes in the LSB of the last byte of that segment.

Table 3: Information encoding in a cover image

Pixel	1	---	---	---	151 byte 01101011
	152	---	---	---	302 byte 10110100
	303	---	---	---	453 byte 11001011
	454	---	---	---	605 byte 11000101

3.3. Decoding message from cover image

The following algorithm is used to decode the message from the cover image,

Information Decoding_Algorithm (N,n,s,msg,img)

```
1.  msg ←fetch[N]
2.  K← 1
3.  Repeat step 4 while N= = n.
4.  Repeat step 5 for i ← 1 to r
5.  Repeat step 6 for j ←1 to c
6.  Count ←count+1
7.  If count = = s
7.1 fetch[K] ← Img[I,j]
7.2 K ← K+1
8.  Return
```

3.4. Working of decoding algorithm

An array k is declared to store the information bit that is fetched by this algorithm from the cover image. If the size of the secret message in bits (N) is equal to the number of segments. Then a loop 'i' works from 1 to row and 'j' loop works from 1 to column, place each iteration in count variable until the count is equal to segment size(S). When it reaches its size, it fetches the LSB of that last byte of the segment and store in the array k.

In Table 4, the first segment is from 1 to 151 bytes and in last bit of last byte secret message bit is hidden. That is retrieved by this algorithm easily (Fig. 3). Fig. 4 shows the working flow of decoding algorithm.

Table 4: Information decoding from the cover image

Pixel	1	---	---	---	151 byte 01101011
	152	---	---	---	302 byte 10110100
	303	---	---	---	453 byte 11001011
	454	---	---	---	605 byte 11000101
	606	---	---	---	----

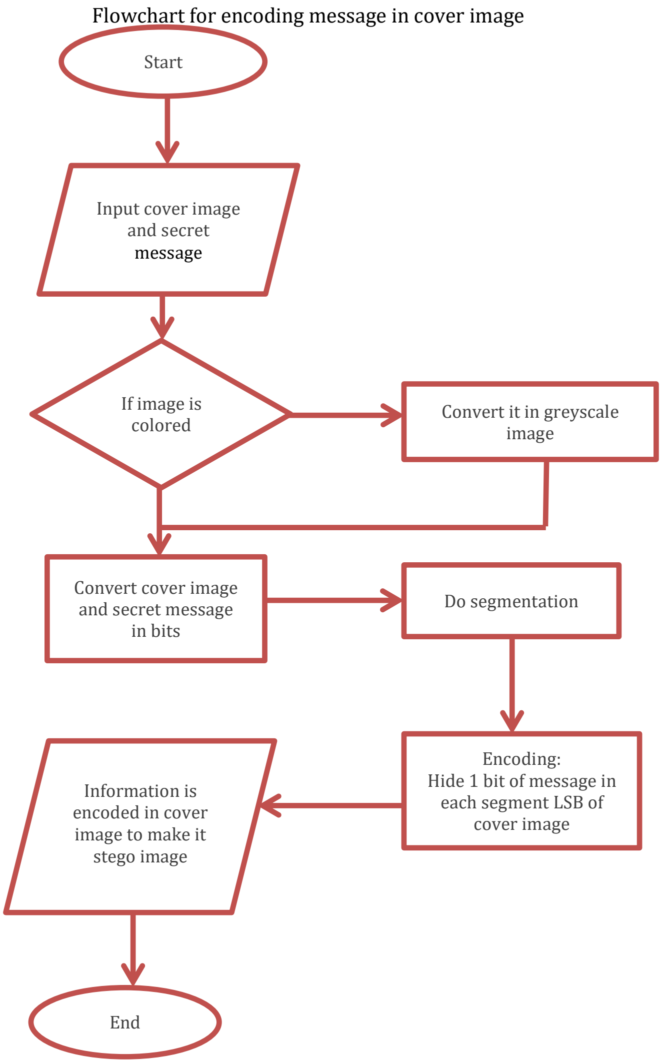

Flowchart for encoding message in cover image
Start
Input cover image and secret message
If image is colored
Convert it in greyscale image
Convert cover image and secret message in bits
Do segmentation
Encoding: Hide 1 bit of message in each segment LSB of cover image
Information is encoded in cover image to make it stego image
End

Fig. 3: A pictorial representation of information encoding

4. Application representation (result)

This application is developed to check the effectiveness and validity of this proposed approach. As a result, empirical results were generated; these steps cover the experimental part of this research. Following snapshot describe the working of this system:

- Firstly click on the following picture will appear where two buttons are placed to use as embed text and decode text (Fig. 5).

Flowchart of decoding message from cover image

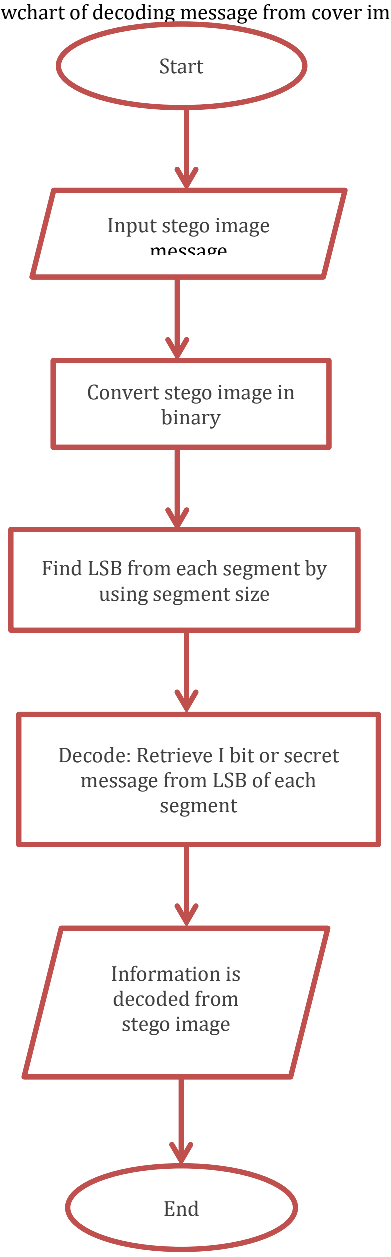

Start
Input stego image message
Convert stego image in binary
Find LSB from each segment by using segment size
Decode: Retrieve I bit or secret message from LSB of each segment
Information is decoded from stego image
End

Fig. 4: Pictorial representation of information decoding

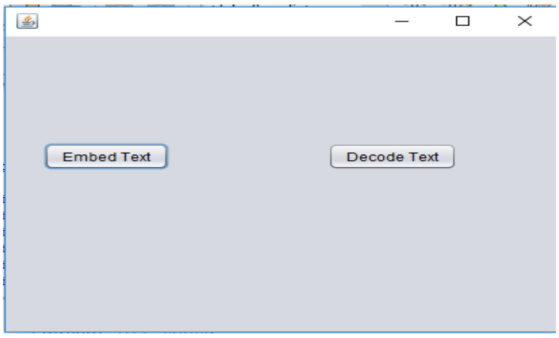


Fig. 5: Form to embed text

- Click on the button "embed text." The following window will appear (Fig. 6).
- This title bar displays the purpose of this window. "Embed steganography message in the image" Below the title bar text bar is displayed where the text is written that anyone wants to transmit secretly to the destination by embedding in an image. Like the following (Fig. 7).

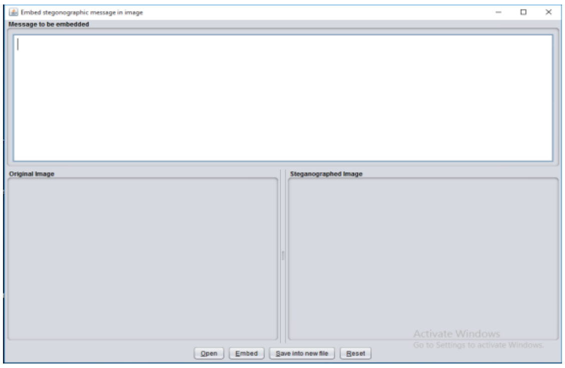
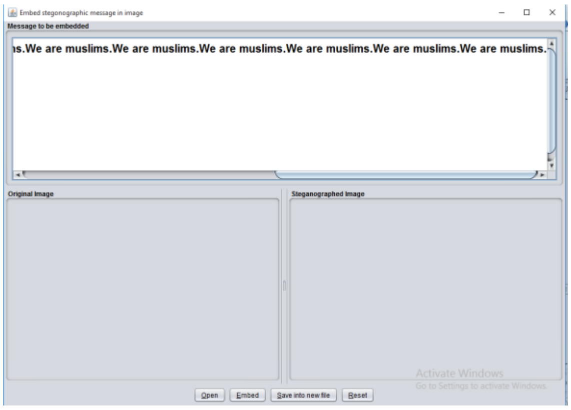


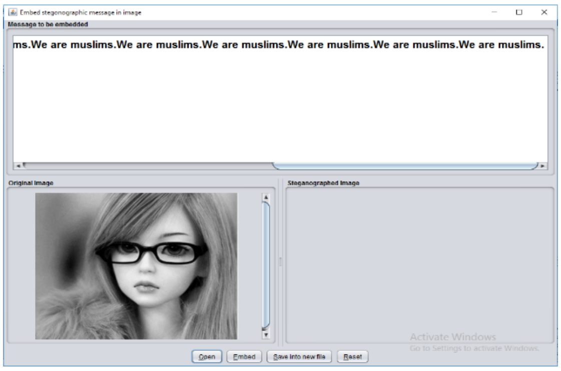
Fig. 6: Form to write text



ıs.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.

Fig. 7: Form to open a picture file

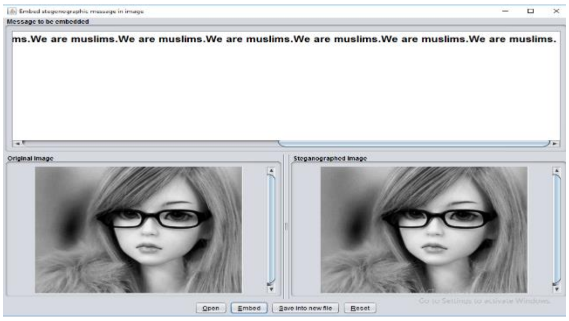
- At the bottom, four buttons are placed "open", "embed", "save into a new file" and "reset." When clicking on "Open button" the following window appears (Fig. 8).



ms.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.

Fig. 8: Form to display a selected image

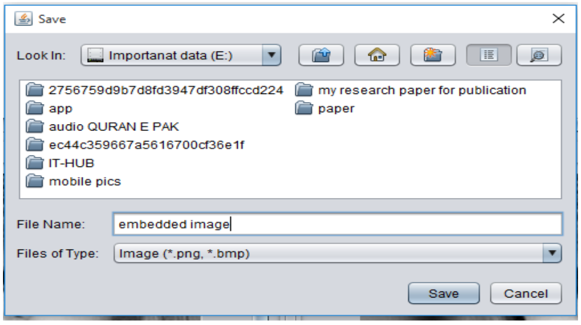
In this study, if a color image is selected to hide data that color image is firstly converted in grey scale image and display as black n white instead of color, because of the security purpose. If data is hidden in the pixels of the image than actual data of image pixel is changed. These variations are too slightly in the grayscale image and can't be judged by naked eye easily as compared to color. After that click on the button "embed" than written text is embedded in the image than the image is displayed in another box of stego image (Fig. 9).



Message to be embedded: ms.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.We are muslims.

Fig. 9: Form to show embedded image

- Now save this image as an embedded text image or stego image (Fig. 10).


Save
2756759d9b7d8fd3947df308ffccd224
app
audio QURAN E PAK
ec44c359667a5616700cf36e1f
IT-HUB
mobile pics
my research paper for publication
paper
Save
Cancel

Look In: Importanat data (E:)

File Name: embedded image

Files of Type: Image (*.png, *.bmp)

Fig. 10: Form to save an embedded image

- Now the image is saved as stego image that is decoded as follows by clicking on the decode button (Fig. 11).

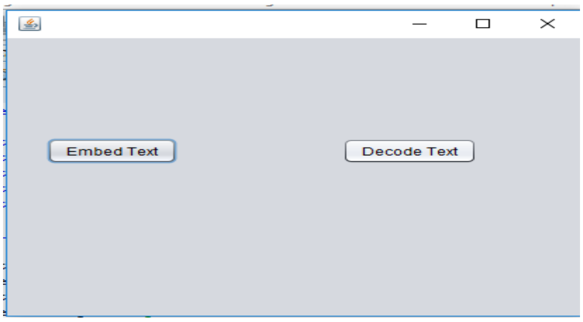


Fig. 11: Form to show decode button

- Click on the decode button. Following window appears (Fig. 12).

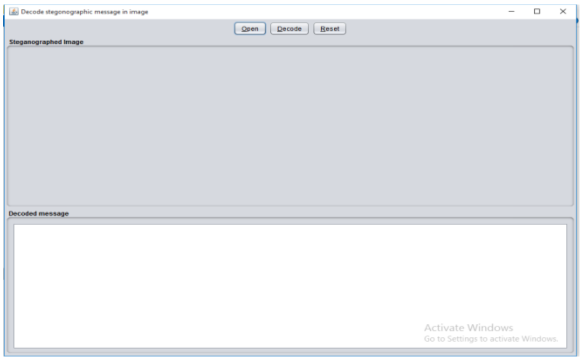
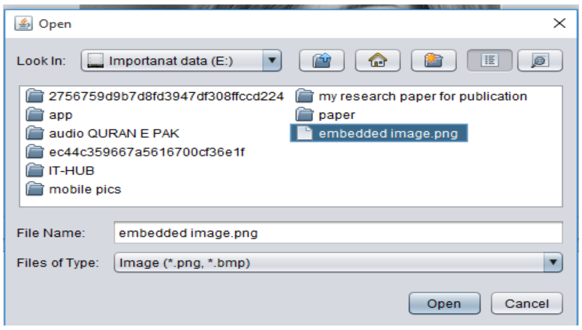


Fig. 12: Form to open embedded image

- After clicking on the open button, the following form appears where we select the image in which data is hidden (Fig. 13).


Open
2756759d9b7d8fd3947df308ffccd224
app
audio QURAN E PAK
ec44c359667a5616700cf36e1f
IT-HUB
mobile pics
my research paper for publication
paper
embedded image.png
Open
Cancel

Look In: Importanat data (E:)

File Name: embedded image.png

Files of Type: Image (*.png, *.bmp)

Fig. 13: Form to open embedded image

- After clicking on this open button required image is opened as follows (Fig. 14).

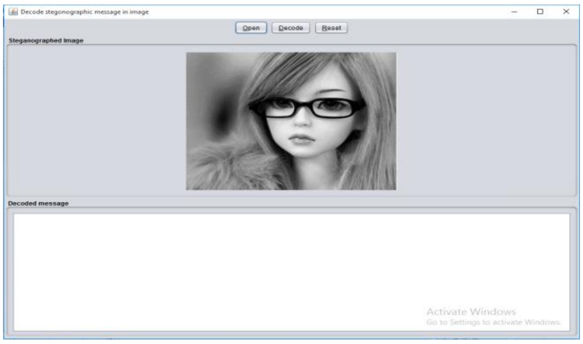
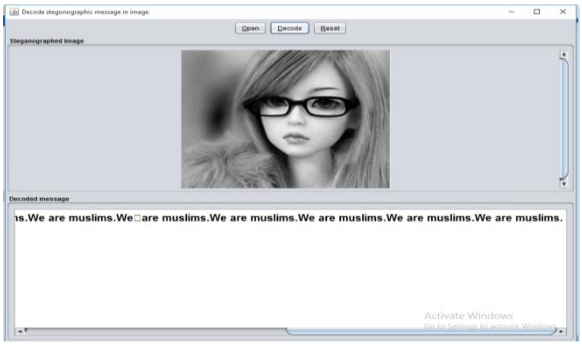


Fig. 14: Form to open embedded image

- After that, we click on the decode button than hidden information becomes visible (Fig. 15).



Decoded message: ıs.We are muslims.We□are muslims.We are muslims.We are muslims.We are muslims.We are muslims.

Fig. 15: Form to open embedded image

- Now click on reset button to go back to embed new data (Fig. 16).

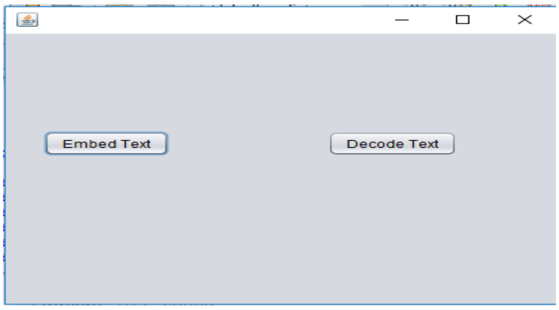


Fig. 16: Form to embed new data

5. Conclusion

This proposed technique is better than previous method because it utilizes full image to hide information by using the segmentation approach that divides image according to the information size in bits, so there is no image degradation and no fade or blurs color issues. This approach also makes it more secure and robust because of its image quality, which is remaining same so nobody is capable of guessing the existence of information in it. This proposed technique fulfils the requirements of steganography like imperceptibility, security and robustness, etc.

6. Future work

In future, this technique is used in a social application for secure chatting purpose. Where any image would be required to write the message that the image is delivering to a receiver that is received by a person who also has same application installed in mobile but to open the image he required a password that is sending by the sender. This approach has a deficiency in case of image size that can be resolve in my future work by some encryption or other technique. When message size is small then, a number of segments would be less and maintain the image quality.

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

References

Alam FI, Bappee FK, and Khondker FU (2011). An investigation into encrypted message hiding through images using LSB. International Journal of Engineering Science and Technology, 3(2): 948-960.

Avcibas I, Memon N, and Sankur B (2003). Steganalysis using image quality metrics. IEEE Transactions on Image Processing, 12(2): 221-229. https://doi.org/10.1109/TIP.2002.807363 **PMid:18237902**

Balgurgi PP and Jagtap SK (2012). Intelligent processing: An approach of audio steganography. In the International Conference on Communication, Information and Computing Technology, IEEE, Mumbai, India: 1-6. https://doi.org/10.1109/ICCICT.2012.6398182

Bawaneh MJ and Obeidat AA (2016). A secure robust gray scale image steganography using image segmentation. Journal of Information Security, 7(3): 152-164. https://doi.org/10.4236/jis.2016.73011

Changder S, Debnath NC, and Ghosh D (2009). A new approach to Hindi text steganography by shifting matra. In the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, IEEE, Kottayam, Kerala, India: 199-202. https://doi.org/10.1109/ARTCom.2009.122

Gadiparthi M, Sagar K, Sahukari D, and Chowdary R (2011). A high capacity steganographic technique based on LSB and PVD modulus methods. International Journal of Computer Applications, 22(5): 8-11.

Hussain M and Hussain M (2013). A survey of image steganography techniques. International Journal of Advanced Science and Technology, 54: 113-124.

Juneja M and Sandhu PS (2009). Designing of robust image steganography technique based on LSB insertion and encryption. In the International Conference on Advances in Recent Technologies in Communication and Computing, IEEE, Kottayam, Kerala, India: 302-305. https://doi.org/10.1109/ARTCom.2009.228

Manjula GR and Danti A (2015). A novel hash based least significant bit (2-3-3) image steganography in spatial domain. International Journal of Security, Privacy and Trust Management, 4(1): 11-20.

Nilizadeh AF and Nilchi ARN (2013). Steganography on RGB images based on a "Matrix Pattern" using random blocks. International Journal of Modern Education and Computer Science, 5(4): 8-18. https://doi.org/10.5815/ijmecs.2013.04.02

Pftizmann B (1996). Information hiding terminology-results of an informal plenary meeting and additional proposals. In the First International Workshop on Information Hiding, Springer-Verlag, Berlin, Germany, 1174: 347-350.

Rahman MM, Mondal PK, Mandal I, and Sultana H (2016). Secure RGB image steganography based on triple-a algorithm and pixel intensity. International Journal of Scientific and Engineering Research, 7(3): 864-869.

Rosaline SI and Raj MA (2013). Adaptive pixel pair matching based steganography for audio files. In the International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, IEEE, Tiruvannamalai, India: 1-5. https://doi.org/10.1109/ICEVENT.2013.6496572 **PMid:23956540 PMCid:PMC3740649**

Shrivastava A and Singh L (2016). A new hybrid encryption and steganography technique: A survey. International Journal of Advanced Technology and Engineering Exploration, 3(14): 9-14. https://doi.org/10.19101/IJATEE.2016.314005

Sravanthi GS, Devi BS, Riyazoddin SM, and Reddy MJ (2012). A spatial domain image steganography technique based on plane bit substitution method. Global Journal of Computer Science and Technology Graphics and Vision. 12(15): 176-179.

Tiwari N, Sandilya M, and Chawla M (2014). Spatial domain image steganography based on security and randomization. International Journal of Advanced Computer Science and Applications, 5(1): 156-159. https://doi.org/10.14569/IJACSA.2014.050121

Umamaheswari M, Sivasubramanian S, and Pandiarajan S (2010). Analysis of different steganographic algorithms for secured data hiding. IJCSNS International Journal of Computer Science and Network Security, 10(8): 154-160.

Vishal W (1992). Bryon, Linear, color separablehuman visual system model for vector diffusioning system. Journal of Electronic Imaging, 1: 277-292.

Viswanatham VM and ManikondaJ (2010). A novel technique for embedding data in spatial domain. International Journal on Computer Science and Engineering, 2(2): 233-236.

Zhang HJ and Tang HJ (2007). A novel image steganography algorithm against statistical analysis. In the International Conference on Machine Learning and Cybernetics, IEEE, Hong Kong, China, 7: 3884-3888. https://doi.org/10.1109/ICMLC.2007.4370824