Research Article GU J Sci34(3): 748-763 (2021) DOI: 10.35378/gujs.703803

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

Image Steganography-Based GUI Design to Hide Agricultural Data

Serdar SOLAK[1,*], Umut ALTINISIK[2]

[1]*Kocaeli University, Faculty of Technology, Information Systems Engineering Department, 41001, Kocaeli, Turkey*
[2]*Kocaeli University, Informatics Department, 41001, Kocaeli, Turkey*

Highlights

- Designed image steganography-based GUI to hide and extract agricultural data.
- Integrated four different steganography techniques in designing the GUI.
- Provided extra security so that hidden agricultural data can’t be accurately decrypted.
- This is the first study performed on image steganography using agricultural databases.

Article Info

Received: 16 Mar 2020
Accepted: 02 Dec 2020

Keywords

Image steganography
LSB substitution
PVD
Data hiding
Agriculture data

Abstract

Throughout the ages, safely preserving and transmitting data that have extraordinary importance for humanity has increased its importance with rapid advances in computer technology. Steganography stores hidden data within the files, which are unnoticed by third parties, so it provides secure transmission of data to the receiver. In this study, a steganography-based GUI design has been carried out, which ensures that the agricultural data is safely stored and communicated to the other party. We used LSB one-bit, two-bit, three-bit substitution and PVD algorithms with GUI for stages of agricultural data hiding and extracting at cover images. We also provided extra security using the embedded key and shifting operations on the hidden data before hiding data the cover image. In short, we confused the hidden data in the cover image so that malicious people can't understand. In experimental studies, performance analysis was evaluated by comparing various criteria as similarity ratio (Structural Similarity Index Measure, SSIM), stego image quality (Peak Signal-to-Noise Ratio, PSNR) and data hiding capacity (Payload).

1. INTRODUCTION

The data created in the digital systems have reached significantly in recent years. These big data are processed by popular computer technologies such as deep learning [1], image detection and recognition [2,3], data mining [4], machine learning [5] and artificial intelligence [6] to be used in several fields such as health [7], education, sports and agriculture [8-11]. The impact of the technological developments in the field of agriculture has led to the emergence of smart farming systems [12-14] as a new popular field. Smart farming systems play an effective role in agricultural productivity, sustainability, environmental factors and food safety [15]. Data security should be ensured when data acquisition, storage and communication between sensors in smart farming applications.

Nowadays, digital technology and the internet are widely used, so confidentiality of data should be ensured in the end-to-end communication and prevented the malicious attacks. Data encryption and data hiding techniques are usually used to prevent the security problem that will arise. Cryptography [16,17] is the technique of data encryption using mathematical equations to provide data integrity, security, privacy and identity control [18]. Steganography [19,20] is a data hiding technique used to embed secure data into various file types, which is unnoticed by third parties [21,22]. Herodotus, who was one of the first to mention the concept of steganography, wrote a secret message to a slave's scalp, and when his hair lengthened, he sent the message to the other side without being noticed. For this instance, a human head is chosen as the transmission medium of the message, and the message becomes unnoticeable to the third party by the regrowing of hair [23].

*Corresponding author, e-mail:serdars@kocaeli.edu.tr

The main purpose of steganography is to securely hide the data to be sent to the other party in data communication in the several file formats which are text, audio, video or image. The data are hidden in the images and transmitted to the other parties, called image steganography [24]. When image steganography is used, a large amount of data can be embedded in an innocent image on the internet without the knowledge of people. Least Significant Bit Substitution (LSB) is one of the most widespread methods that can be easily realized to hide data [18,25]. The LSB substitution method is used in different ways in the literature [21,26-29]. Pixel-Value Differencing (PVD) is another method commonly used in image steganography [30]. PVD method hides high-capacity data into the cover image more securely than one-bit LSB technique. The LSB method and PVD technique or the similar techniques are utilized together in the literature, and obtained high stego image quality, more capacity, and more secure.

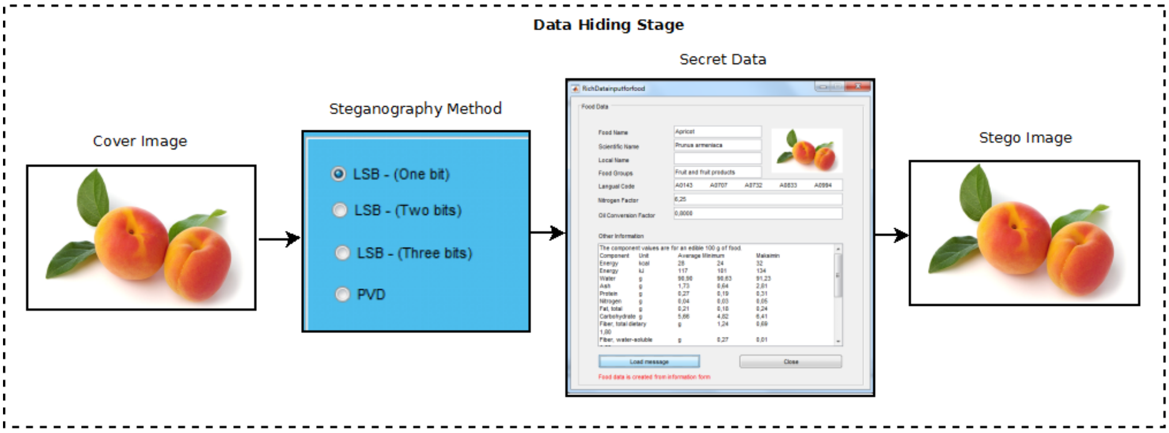
In recent years, many studies have been conducted to improve the capacity, safety and stego image quality using PVD-based methods [31-36]. In the article, GUI which makes it easy to hide the data in the agricultural databases to cover images and extract the hidden data from the stego image was designed to effectively use image steganography in the field of agriculture. We used The National Gardening Association Database [37] and Turkish Food Composition Database [38]. In the Plants Database jointly developed by more than 3,500 Garden.org members from around the world, there are 735,395 plants and 543,804 images. Turkomp which contains data from 580 foods from 14 food groups, was created, because of the pilot studies conducted under the European Food Information Resource [39] project by [40] The process of hiding and extracting agricultural data obtained from Plants and Turkomp databases using GUI can be performed according to four different algorithms. In the GUI, the data obtained from the files, which were saved in these files from the agricultural database, were hidden in the cover images, as well as a new form was designed for Turkomp database to utilize effectively. In experimental studies, the data from Turkomp or Plants database are hidden in the cover image file in which the original size of it, which had both data and image, remained unchanged. We can conclude that the main contributions of our study presented in this article are as follows:

- We have designed image steganography-based GUI to hide and extract agricultural data,
- We have integrated four different steganography techniques in designing the GUI,
- We have used the optimized versions of integrated steganography methods,
- We have provided extra security by using an embedded key and shifting so that hidden agricultural data cannot be accurately decrypted by third parties,
- This is the first study performed on image steganography using agricultural databases.

The rest of the article is arranged as follows. In Section 2, data hiding and data extracting are presented in detail for LSB substitution one-bit, two-bit, three-bit and PVD methods. In Section 3, we design image steganography-based GUI to hide and extract data in the agricultural field. In Section 4, the experimental study's results are presented and analyzed. Finally, conclusions and future studies are presented in Section 5.

2. MATERIAL METHOD

Image steganography consists of two stages as data hiding and data extraction. In our paper, the hiding of data takes place in four stages, while the extraction of data is generated in three stages. The data hiding stage involves retrieving the cover image, selecting the image steganography method, creating the secret using the agricultural database and obtaining the stego image. In the image steganography, the image where the data are hidden is called a cover image, which is loaded from the camera or agricultural databases. To determine how the data are hidden to the cover image is called the steganography method which is used as LSB substitution one-bit, two-bit, three-bit, and PVD method. Then, the data from the agricultural databases constitute secret data, which is encrypted. Finally, stego image which the hidden data is contained is generated using image steganography methods and secret data. Figure 1 presents the block diagram of the data hiding method used in this paper.



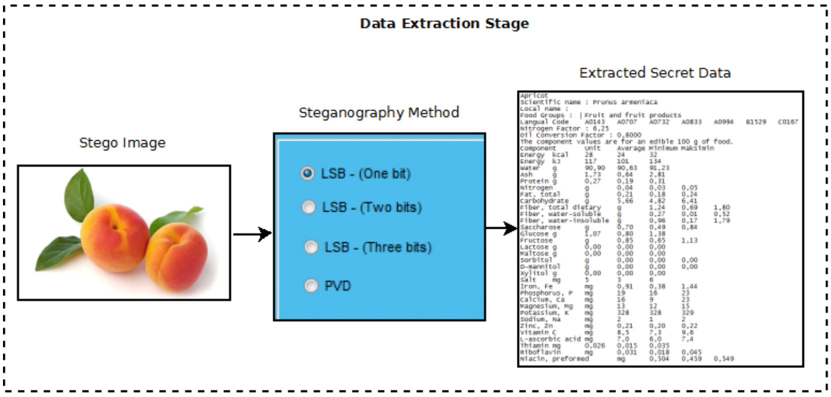
Food Name: Apricot
Scientific Name: Prunus armeniaca
Local Name:
Food Groups: Fruit and fruit products
Langual Code: A0143 A0707 A0732 A0833 A0994
Nitrogen Factor: 6,25
Oil Conversion Factor: 0,8000
Other Information:

```
The component values are for an edible 100 g of food.
Component      Unit      Average Minimum      Maksimin
Energy         kcal      28          24          32
Energy         kJ        117         101         134
Water          g         90,90       90,63       91,23
Ash            g         1,73        0,64        2,81
Protein        g         0,27        0,19        0,31
Nitrogen       g         0,04        0,03        0,05
Fat, total     g         0,21        0,18        0,24
Carbohydrate   g         5,66        4,82        6,41
Fiber, total dietary     g           1,24        0,69
1,80
Fiber, water-soluble     g           0,27        0,01
```

Food data is created from information form

***Figure 1.** Block diagram of data hiding stage*

The data extraction stage includes the stego image, selecting the image steganography method, and obtaining the data. The stego image is used as the input in the data extraction stage. To extract the data from the stego image, the appropriate steganography method, which was used to hide the data, must be chosen. The decryption process is performed on the extracted secret data, and finally the agricultural data are obtained. Figure 2 shows the block diagram of the data extraction method used in our paper.



```
Apricot
Scientific name : Prunus armeniaca
Local name :
Food Groups :  |Fruit and fruit products
Langual Code    A0143   A0707   A0732   A0833   A0994   B1529   C0167
Nitrogen Factor : 6,25
Oil Conversion Factor : 0,8000
The component values are for an edible 100 g of food.
Component       Unit    Average Minimum Maksimin
Energy  kcal    28      24      32
Energy  kJ      117     101     134
Water   g       90,90   90,63   91,23
Ash     g       1,73    0,64    2,81
Protein g       0,27    0,19    0,31
Nitrogen        g       0,04    0,03    0,05
Fat, total      g       0,21    0,18    0,24
Carbohydrate    g       5,66    4,82    6,41
Fiber, total dietary    g       1,24    0,69    1,80
Fiber, water-soluble    g       0,27    0,01    0,52
Fiber, water-insoluble  g       0,96    0,17    1,79
Saccharose      g       0,70    0,49    0,84
Glucose g       1,07    0,80    1,38
Fructose        g       0,85    0,65    1,13
Lactose g       0,00    0,00    0,00
Maltose g       0,00    0,00    0,00
Sorbitol        g       0,00    0,00    0,00
D-mannitol      g       0,00    0,00    0,00
Xylitol g       0,00    0,00    0,00
Salt    mg      5       3       6
Iron, Fe        mg      0,91    0,38    1,44
Phosphorus, P   mg      19      16      23
Calcium, Ca     mg      16      9       23
Magnesium, Mg   mg      13      12      15
Potassium, K    mg      328     328     329
Sodium, Na      mg      2       1       2
Zinc, Zn        mg      0,21    0,20    0,22
Vitamin C       mg      8,5     7,3     9,6
L-ascorbic acid mg      7,0     6,0     7,4
Thiamin mg      0,026   0,015   0,035
Riboflavin      mg      0,031   0,018   0,045
Niacin, preformed       mg      0,504   0,459   0,549
```

***Figure 2.** Block diagram of the data extraction stage*

2.1. LSB Substitution

LSB substitution is one of the easiest methods to perform and use in image steganography. The main principle is based on changing the least significant bits of the pixel values that comprise the cover image. The LSB substitution method has low computational complexity. However, when the amount of the secret data is too large, the probability of detecting the data in the stego image increases. The LSB substitution method is performed as LSB one-bit, two-bit and three-bit to hide the agricultural data in the cover images.

2.1.1. Data hiding process of LSB substitution

The agricultural data hiding process is described for LSB substitution one-bit, two-bit and three-bit, respectively. In the LSB substitution one-bit method, while the data is hidden in the colored cover image, the least significant last bit of each color channel is changed. The data hiding process is usually sequenced as RGBRGBRG for eight-bit data. In this study, we use different hiding sequences that are difficult to understand by third parties such as RGBBGRRG and RRRGGGBB, while agricultural data are hidden in the colored cover image. Figure 3 shows a block diagram of the LSB substitution one-bit used RGBBGRRG sequentially. The block diagram illustrates that the letter ‘S’ is hidden in the first three pixels of the sunflowers cover image. While the LSB substitution one-bit method is applied, the cover image pixel values and secret data are converted to binary values. To create a stego image, we apply logical ‘AND’ or ‘OR’ operation to least significant bit of the cover image pixel when the bit value of the secret data is 0 or 1. Thus, three bits of data are hidden in one pixel of the cover image.

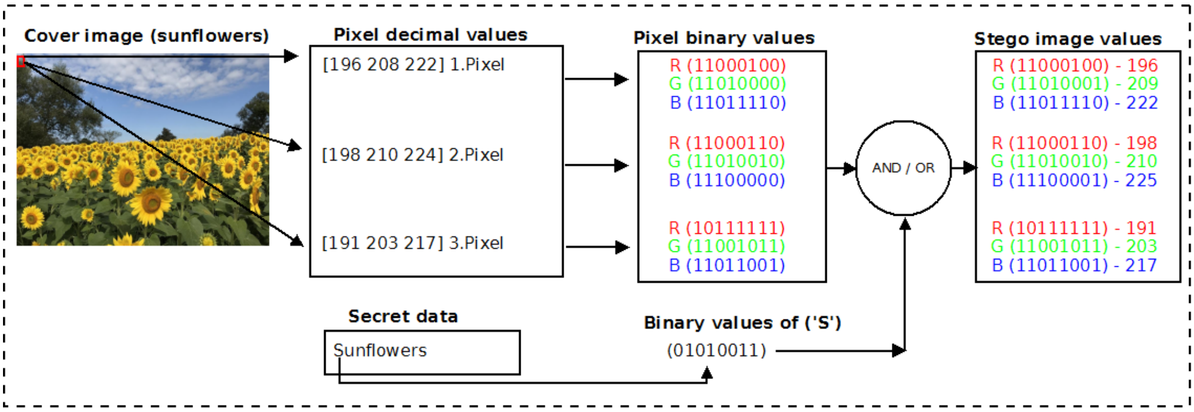


Figure 3. *Block diagram of LSB substitution one-bit*

In the LSB substitution two-bit method, the data hiding process is performed by replacing the least significant two bits of the colored cover image. Although up to six-bit data is hidden in one pixel of the colored cover image, four-bit data are usually hidden in the literature studies using this method [21,41-42]. The red (R), green (G), and blue (B) color channels can hide maximum six-bit data by using last two-bit data, or four-bit data are hidden using different versions as R2G2, G2B2, R2B2, R2G1B1 etc. As a result of our experimental studies, we realize the method that we call the LSB 211 hides two bits of data into the red channel and one bit of data to both green channel and blue channel, which provides high similarity ratio between cover image and stego image. Figure 4 shows the block diagram of LSB substitution two-bit as LSB211. Four-bit data is hidden in one pixel of the cover image using the logical 'AND' and 'OR' operations as in LSB substitution one-bit.

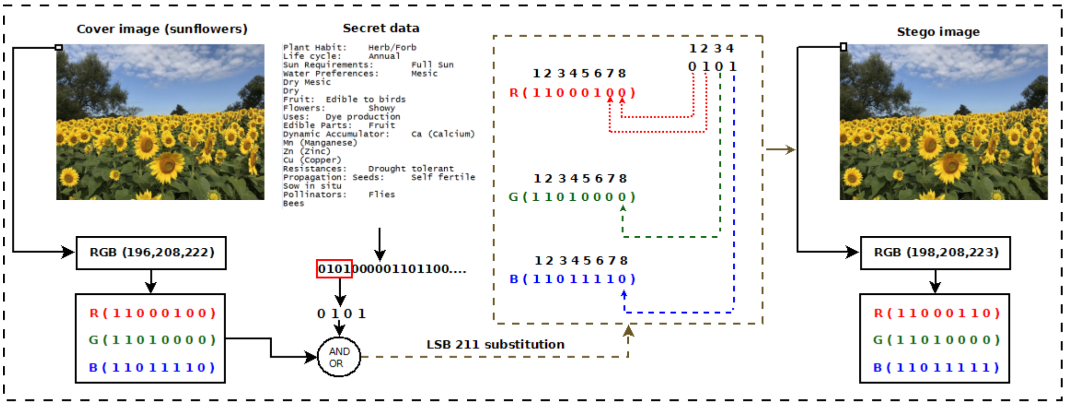


Figure 4. *Block diagram of LSB substitution two-bit as LSB211*

In the LSB substitution three-bit method, the data is hidden in the colored cover image with the replacement of the least significant three-bit. Maximum nine-bit data is hidden in one pixel of the colored cover image by LSB substitution three-bit. Our prior studies indicate that the LSB332 produces a high quality stego image according to the other LSB substitution three-bit methods as LSB233 and LSB323, so we use the LSB332 to hide data [26]. Figure 5 shows the block diagram of LSB substitution three-bit as LSB332. The LSB332 utilizes three-bit of the red channel and green channel and two-bit of the blue channel, so a total of eight-bit secret data is hidden. Figure 5 presents a data hiding example, which illustrates how to hide the first eight-bit secret data from the Plants database to the sunflowers cover image. The first pixel of the sunflowers cover image is presented in RGB values, respectively 196, 208 and 222. When the first eight-bit secret data (01010000) is hidden in this pixel by the LSB332, the stego image pixel values are the RGB values respectively 194, 209 and 220. It is not possible to perceive by the human eye the change in color values because of the data hiding process. In this way, agricultural data in the stego image cannot be perceived by the people. In the study, when LSB substitution one-bit, two-bit and three-bit are used, the

512x512 size of the colored cover images can be hidden agricultural data by approximately 85 KB, 128 KB and 256 KB, respectively.

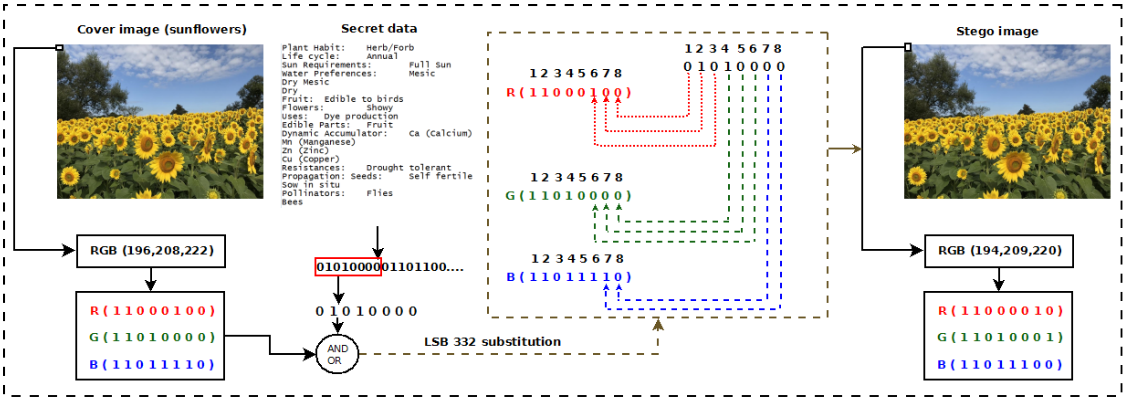


Figure 5. Block diagram of LSB substitution three-bit as LSB332

2.1.2. Data extraction process of LSB substitution

We present the extraction of the data in the stego image in this section. Stego image which contains agricultural data hidden by LSB substitution methods is used as input. Equation (1) is the formula that shows the extraction of agricultural data from the stego image. When the X, Y and Z values in the equation are 1 in the LSB substitution one-bit, differ according to in LSB substitution two-bit and three-bit methods. For instance, LSB211 includes X = 2, Y = 1 and Z = 1, while LSB332 covers X = 3, Y = 3 and Z = 2. In Equation (1), bR, bG and bB symbols are numerical data obtained from red, green and blue channels and $P^{'}$ refers to the pixel value of stego image. The obtained bR, bG and bB binary values are evaluated according to hiding sequences and agricultural data is extracted,

$$(b_R,b_G,b_B)=\left(\left(P^{'}_R \bmod 2^X\right),\left(P^{'}_G \bmod 2^Y\right),\left(P^{'}_B \bmod 2^Z\right)\right). \qquad (1)$$

2.2. PVD

PVD which is one of the methods commonly used in image steganography, performs data hiding, taking into consideration the difference between two adjacent pixel values. PVD hides agricultural data that include between three-bit and seven-bit in two adjacent pixels. There are high color differences between adjacent pixels in the edge regions, so more data is hidden in them. The PVD consequently proposes a reasonably good quality stego image and high capacity data [20].

2.2.1. Data hiding process of PVD

This section describes the hiding of agricultural data on the colored cover image by the PVD method. The color channel values of the adjacent two pixels (Pi, Pi+1) are used in the process of hiding the data. According to the absolute difference (dc) between cover image pixel values, the amount of data (t) is determined, which is hidden in each color channel. In Table 1, the lower and upper band ranges are used to determine the amount of data to hide. To calculate bit capacity, Equation (2) is used,

$$t=\log_2(\text{upper-lower}+1). \qquad (2)$$

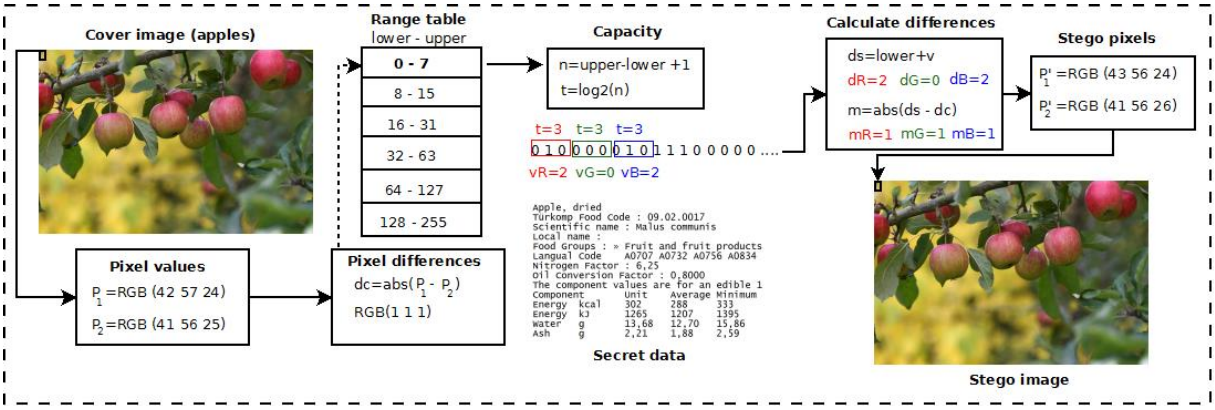
Table 1. *PVD range table*

	Range 1	Range 2	Range 3	Range 4	Range 5	Range 6
Lower band	0	8	16	32	64	128
Upper band	7	15	31	63	127	255
Bit capacity (t)	3	3	4	5	6	7

The ASCII value of the characters is converted to the binary system and the bit string of all the secret data is generated. Data up to the capacity of t for each color channel which determined is taking from this bit string and decimal number (v) is calculated. The sum of the calculated v and lower band value gives the two adjacent pixel differences (ds) that will create the stego image. To find the two adjacent pixel values (P'_i,P'_{i+1}) in the stego image, the absolute difference (m) between the dc and the ds is calculated. In Equation (3), when calculating the pixel values of the stego image, Pi, Pi+1, dc, ds and m values are used [22,35]

$$(P'_i,P'_{i+1})=\left\{\begin{matrix} ((P_i\geq P_{i+1})\ \&\ (d_s\leq d_c))\rightarrow P_i-\left\lceil\frac{m}{2}\right\rceil, P_{i+1}+\left\lfloor\frac{m}{2}\right\rfloor \\ ((P_i<P_{i+1})\ \&\ (d_s>d_c))\rightarrow P_i-\left\lfloor\frac{m}{2}\right\rfloor, P_{i+1}+\left\lceil\frac{m}{2}\right\rceil \\ \text{others}\rightarrow P_i+\left\lceil\frac{m}{2}\right\rceil, P_{i+1}-\left\lfloor\frac{m}{2}\right\rfloor \end{matrix}\right\}. \tag{3}$$

Figure 6 shows the block diagram of the PVD method. The first nine-bit (010000010) of the secret data is hidden on the first two adjacent pixels of the apples cover image in the block diagram. The first two adjacent pixel values of the cover image are RGB (42, 57, 24) and RGB (41, 56, 25), whereas the first two adjacent pixel values that occur in the stego image are RGB (43, 56, 24) and RGB (41, 56, 26). As seen from the example in the block diagram, although the nine-bit part of the secret data is hidden in the apple cover image, stego image has negligible change that cannot be perceived by the human eye.



```
Apple, dried
Türkomp Food Code : 09.02.0017
Scientific name : Malus communis
Local name :
Food Groups : » Fruit and fruit products
Langual Code     A0707 A0732 A0756 A0834
Nitrogen Factor : 6,25
Oil Conversion Factor : 0,8000
The component values are for an edible 1
Component         Unit    Average Minimum
Energy  kcal      302     288     333
Energy  kJ        1265    1207    1395
Water   g         13,68   12,70   15,86
Ash     g         2,21    1,88    2,59
```

Figure 6. *Block diagram of PVD*

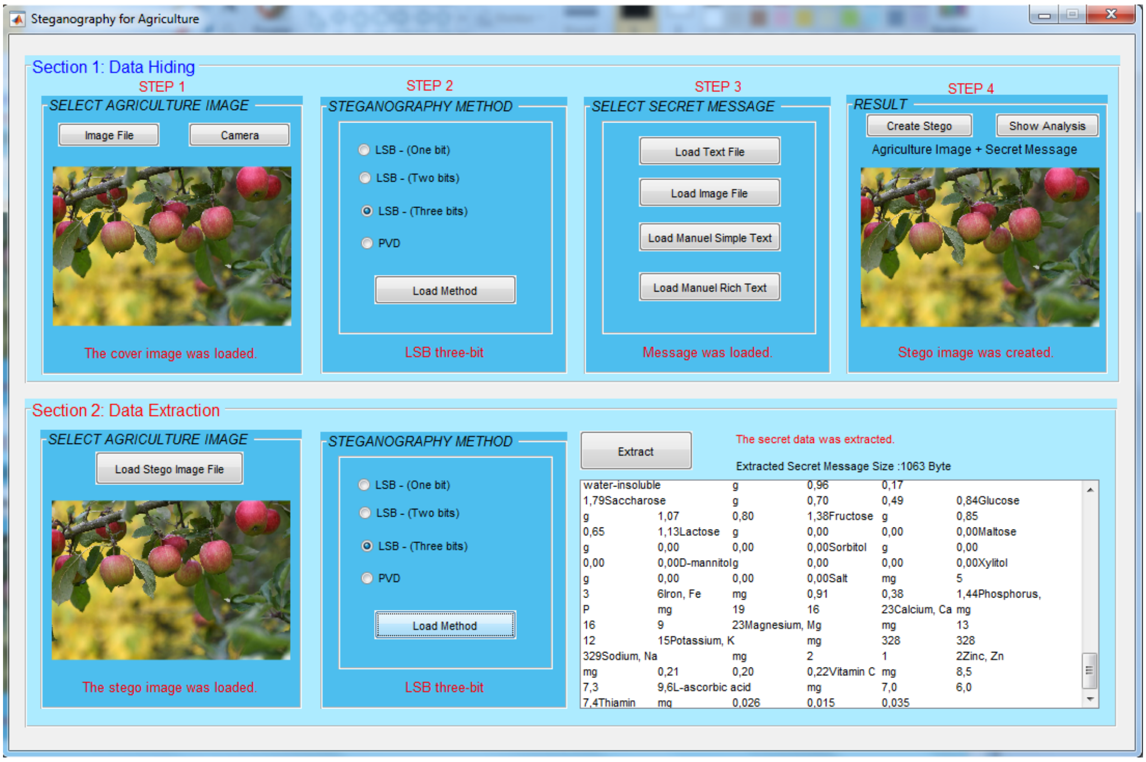
2.2.2. Data extraction process of PVD

This section describes the process of extracting data that are hidden to the cover image using the PVD method. The stego image is the input of the PVD data extraction process. Two adjacent pixel values of the stego image are used in the process of data extraction. We presented extraction procedures by following steps:

Input: W x H size stego image
Output: Secret data
Algorithm
Step 1: Get RGB values of two adjacent pixels (P'_i,P'_{i+1}) from stego image,
Step 2: Calculate the absolute difference between two adjacent pixels (ds=$|P'_i - P'_{i+1}|$),
Step 3: Define upper and lower band values from the range table according to ds value,
Step 4: Calculate the difference between ds and lower band value, and data were obtained,
Step 5: Repeat step 2 to 4 for the green and blue color channels,
Step 6: Repeat step 1 to 5 until the data is finished.

3. GUI DESIGN FOR AGRICULTURAL DATA

Image steganography-based GUI consisting of two parts is prepared using MATLAB software is designed to hide and extract agricultural data. Figure 7 shows designed GUI for agricultural data.



○ LSB - (One bit)
○ LSB - (Two bits)
● LSB - (Three bits)
○ PVD

The cover image was loaded.

LSB three-bit

Message was loaded.

Stego image was created.

The stego image was loaded.

LSB three-bit

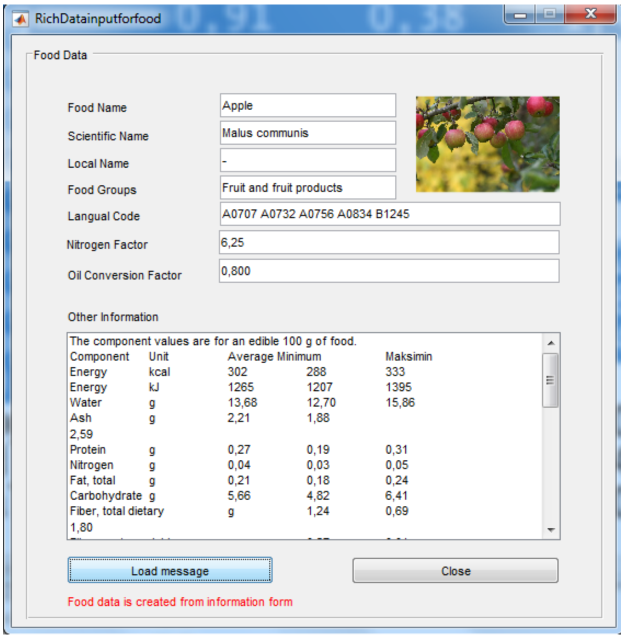
The secret data was extracted.

Extracted Secret Message Size :1063 Byte

```
water-insoluble          g          0,96       0,17
1,79Saccharose           g          0,70       0,49          0,84Glucose
g          1,07          0,80       1,38Fructose g            0,85
0,65       1,13Lactose   g          0,00       0,00          0,00Maltose
g          0,00          0,00       0,00Sorbitol g            0,00
0,00       0,00D-mannitolg          0,00       0,00          0,00Xylitol
g          0,00          0,00       0,00Salt   mg             5
3          6Iron, Fe     mg         0,91       0,38          1,44Phosphorus,
P          mg            19         16         23Calcium, Ca mg
16         9             23Magnesium, Mg       mg            13
12         15Potassium, K           mg         328           328
329Sodium, Na            mg         2          1             2Zinc, Zn
mg         0,21          0,20       0,22Vitamin C mg         8,5
7,3        9,6L-ascorbic acid       mg         7,0           6,0
7,4Thiamin mg            0,026      0,015      0,035
```

Figure 7. Image steganography GUI for agricultural data

The data hiding process is designed as four steps which are taking the cover image, selecting the image steganography method, obtaining data form agricultural database, creating stego image and analysis. Firstly, the cover image is loaded from the camera or file into the GUI.



Food Name	Apple
Scientific Name	Malus communis
Local Name	-
Food Groups	Fruit and fruit products
Langual Code	A0707 A0732 A0756 A0834 B1245
Nitrogen Factor	6,25
Oil Conversion Factor	0,800

```
The component values are for an edible 100 g of food.
Component     Unit        Average Minimum       Maksimin
Energy        kcal        302         288        333
Energy        kJ          1265        1207       1395
Water         g           13,68       12,70      15,86
Ash           g           2,21        1,88
2,59
Protein       g           0,27        0,19       0,31
Nitrogen      g           0,04        0,03       0,05
Fat, total    g           0,21        0,18       0,24
Carbohydrate  g           5,66        4,82       6,41
Fiber, total dietary      g           1,24       0,69
1,80
```

Food data is created from information form

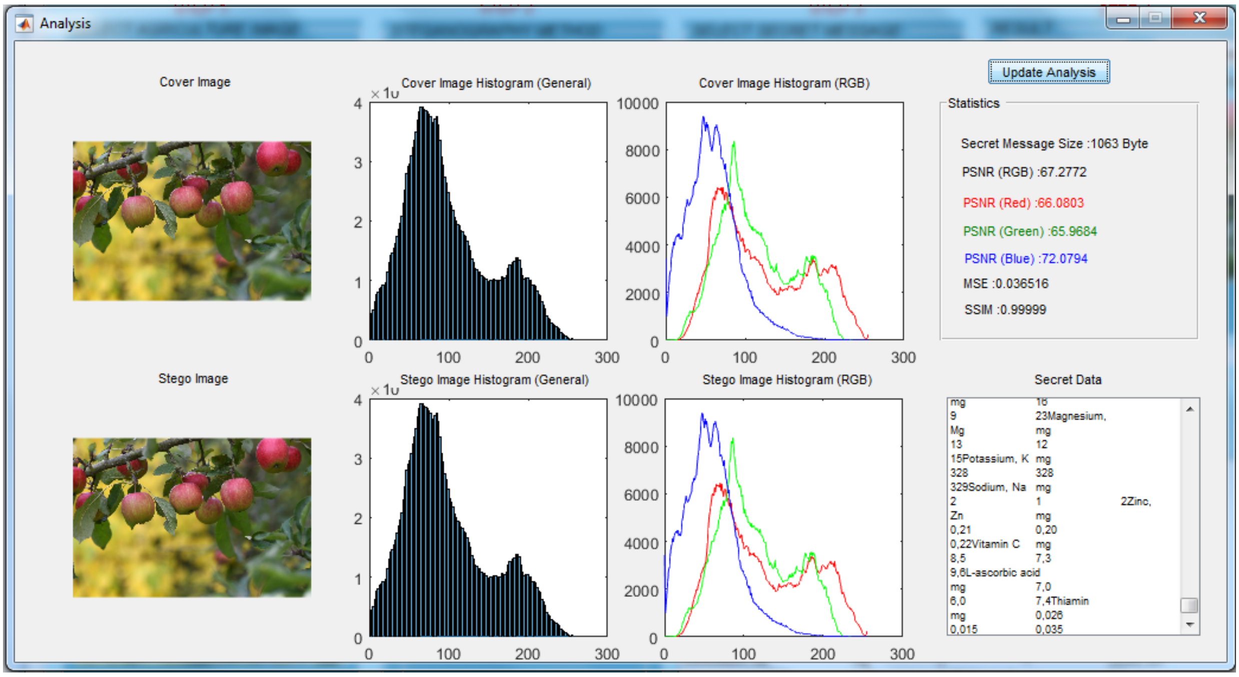
Figure 8. Data form for Turkomp database

The methods which are LSB one-bit, two-bit, three-bit and PVD, which show how to hide the data into the cover image is selected in the second step. In the third step, the data from the agricultural databases is uploaded into the GUI, which is taken as a picture or text file. In addition, we have designed two specific forms, which are called Load Manuel Simple Text and Load Manuel Rich Text, to make the data more efficiently. While the agricultural data is taken from Turkomp database in a special format using Load

Manuel Rich Tex form, simple agricultural data entry is made with Load Manuel Simple Text form. Figure 8 shows the obtained data from the Turkomp database using the Load Manuel Rich Text form.
In the case of hiding agricultural data, extra security procedures are implemented in the GUI which these data can be imperceptible by third parties. In order to ensure safety, embedded key and shifting operations are applied respectively before hiding the agricultural data in the cover image. First, the agricultural data is encrypted using the embedded key. Then, each eight-bit of the encrypted new data is shifted to the left as the number of bits with a value of 1. In this way, secret data are obtained by implementing double layer security. The algorithm that shows the secret data includes the following steps:

Assumption: Embedded key → Agriculture
Input: Message → Apples
Output: Secret Data→*GGC<Vectical Tab>Ý
Algorithm:
Step 1: The ASCII values of 'Agriculture' are obtained. (65, 103, 114, 105, 99, 117, 108, 116, 117, 114, 101),
Step 2: The sum and average of the ASCII values are calculated. (sum=1159, average=105). The embedded key numerical value is calculated using the sum and average. (Embedded key=1159 mod 105, Embedded key=4),
Step 3: The XOR operation is performed between the input data ASCII values ('Apples' – 65, 112, 112, 108, 101, 115) and the Embedded key ASCII value (4) and tempSD (69, 116, 116, 104, 97, 119) is created,
Step 4: The tempSD is converted to a binary number system (01000101, 01110100, 01110100, 01101000, 01100001, 01110111),
Step 5: The number '1' is calculated for each byte of the tempSD binary value (3, 4, 4, 4, 3, 6),
Step 6: In each byte of tempSD, the secret data are obtained by shifting the calculated shift value to the left (00101010, 01000111, 01000111, 01000011, 00001011, 11011101).

In the last step of the data hiding, the stego image, which includes the secret data and the cover image, is created and saved. The Show Analysis page presents the criteria for the performance of the study. In this page, we examine the cover and stego image, general and color channel-based histograms, Peak Signal-to-Noise Ratio (PSNR), the Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM) values, which these criteria are used to measure the quality of the stego image. Figure 9 shows the data analysis page for image steganography. Although the apples cover image comprise 1063 bytes agricultural data from the Plant database, performance criteria are found to be high.


Analysis
Cover Image
Stego Image
Cover Image Histogram (General)
Stego Image Histogram (General)
×10
0
1
2
3
4
0
100
200
300
Cover Image Histogram (RGB)
Stego Image Histogram (RGB)
0
2000
4000
6000
8000
10000
Update Analysis
Statistics
Secret Data

Secret Message Size :1063 Byte
PSNR (RGB) :67.2772
PSNR (Red) :66.0803
PSNR (Green) :65.9684
PSNR (Blue) :72.0794
MSE :0.036516
SSIM :0.99999

```
mg                16
9                 23Magnesium,
Mg                mg
13                12
15Potassium, K    mg
328               328
329Sodium, Na     mg
2                 1                2Zinc,
Zn                mg
0,21              0,20
0,22Vitamin C     mg
8,5               7,3
9,6L-ascorbic acid
mg                7,0
6,0               7,4Thiamin
mg                0,026
0,015             0,035
```

Figure 9. *Data analysis page for image steganography*

The data extraction process is designed as three steps which are taking the stego image, selecting the image steganography method and extracting agricultural data. In the first step, the stego image file where the secret data are hidden is uploaded to the GUI. Then, the image steganography algorithm used in the data hiding step must be selected. Otherwise, it will not be possible to obtain secret data. In the last step, secret data is obtained by using stego image and image steganography method.

In this step, the secret data are first extracted from the stego image, but the extracted secret data are incomprehensible. Because the embedded key and shifting procedures are applied to these data in the data hiding stage. For this reason, the extra security procedures applied in the data hiding process are carried out in reverse order and the data are obtained accurately. In the case that non-stego image is uploaded or an incorrect hiding algorithm is selected, the program generates the error message by detecting it. When sending agricultural data to the receiver using image steganography, it is sufficient that both the sender and the recipient have the same GUI. Even if the stego image can be detected by third parties, it will not be possible to obtain the data correctly because of the extra security in GUI.

4. RESULTS AND DISCUSSION

Experimental studies are carried out with the prepared GUI using the agricultural information and images in the Turkomp, EuroFir and Plant database. Figure 10 shows the different sizes of the colored agricultural cover images in the Plants database used in experimental studies.

(a) Garlic(allium sativum) (b) Apple (malus pumila) (c) Sunflowers (helianthus annuus)

(d) Rose(rosa) (e) Concord grape (vitis labrusca) (f) Tomato (solanum pimpinellifolium)

Figure 10. *The agricultural cover images used in experimental studies*

Table 2 shows the maximum bit capacity that can be embedded in the cover images with image steganography methods used in the study. In LSB methods, the same data capacity is embedded in the same size cover images, while in the PVD method, different data capacity is embedded in each cover image. The reason why different data capacities are embedded is the difference between the two adjacent pixels in the cover image. In Table 2, the LSB three-bit method hides more agricultural data into the cover image than other methods.

Table 2. *Embedding capacity table of the cover images for used image steganography algorithm*

Cover Image	**Size (pixel)**	**Embedding capacity (bits)**			
		LSB one-bit	**LSB two-bit**	**LSB three-bit**	**PVD**
Garlic	1000x667	1778666	2668000	5336000	3164919
Apple	1000x667	1778666	2668000	5336000	3041680
Sunflower	1000x750	2000000	3000000	6000000	3739925
Rose	1000x667	1778666	2668000	5336000	3203320
Grape	1000x664	1770666	2656000	5312000	3210229
Tomato	1000x664	1770666	2656000	5312000	3014133

In the image steganography, the difference between the cover image and the stego image is not perceived by the human eye. Therefore, MSE, PSNR, SSIM and payload evaluation criteria, which are widely utilized in the literature, are employed in the evaluation of experimental studies. The MSE value is calculated using the change between the cover image and the stego image pixel values. Equation (4) provides the formula for calculating MSE. The MSE is calculated for each color channel at the colored cover images and the average of these values is the colored MSE value,

$$\mathrm{MSE}=\frac{1}{\mathrm{WxH}}\sum_{i=1}^{w}\sum_{j=1}^{H}\left(C_{(i,j)}-S_{(i,j)}\right)^{2}. \tag{4}$$

The PSNR [20] value is used to determine the stego image quality. A high PSNR value means that the stego image quality is high. When calculating the PSNR value, the MSE and the maximum pixel value (Max) in the cover image are used. Equation (5) shows the PSNR formula,

$$\mathrm{PSNR}=10\ \mathrm{x}\log_{10}\left(\frac{\mathrm{Max}^{2}}{\mathrm{MSE}}\right). \tag{5}$$

The SSIM is the other evaluation criterion that establishes the similarity of the cover and stego image. Equation (6) shows the calculation of the SSIM [43-45] value,

$$\mathrm{SSIM}(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x{}^2+\mu_y{}^2+c1)(\sigma_x{}^2+\sigma_y{}^2+c2)}. \tag{6}$$

Embedding capacity (payload) is the ratio of the amount of agricultural data to the total number of pixels in the cover image. Equation (7) shows the calculation of the payload (P),

$$\mathrm{P}=\frac{\mathrm{Capacity}}{\mathrm{WxH}}. \tag{7}$$

Table 3. *LSB substitution one-bit performance analysis for message 1 and message 2*

Cover Image	**Embedded message 1 (3560 bits)**						**Embedded message 2 (245792 bits)**					
	MSE	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**	**MSE**	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**
Garlic	0.0009	78.47	77.89	77.97	79.81	1.000	0.061	60.28	59.72	59.78	61.58	0.99985
Apple	0.0009	78.61	77.92	78.21	79.96	1.000	0.061	60.26	59.75	59.72	61.52	0.99995
Sunflower	0.0009	78.92	78.47	78.19	80.45	1.000	0.055	60.75	60.23	60.27	61.97	0.99993
Rose	0.0009	78.61	78.13	78.05	79.88	1.000	0.062	60.21	59.64	59.74	61.48	0.99995
Grape	0.0009	78.62	78.32	78.12	79.54	1.000	0.062	60.20	59.68	59.72	61.44	0.99991
Tomato	0.0009	78.53	78.10	78.07	79.59	1.000	0.062	60.22	59.68	59.72	61.51	0.99978
Average	**0.0009**	**78.63**	**78.14**	**78.10**	**79.87**	**1.000**	**0.061**	**60.32**	**59.78**	**59.83**	**61.58**	**0.99990**

In this paper, the agricultural data obtained from the Plants database are recorded in the files named as message 1 and message 2, then these files are hidden in the cover images and analyzed. Table 3 presents the MSE, PSNR and SSIM values which are obtained by the LSB substitution one-bit used to hide the message 1 and message 2 into the cover images. The average MSE, PSNR and SSIM values for the message1 are calculated as 0.0009, 78.63 and 1 respectively, while it is computed as 0.061, 60.32 and 0.9999 for message 2.

Table 4. *LSB substitution two-bit performance analysis for message 1 and message 2*

Cover Image	**Embedded message 1 (3560 bits)**						**Embedded message 2 (245792 bits)**					
	MSE	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**	**MSE**	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**
Garlic	0.0017	76.15	72.83	79.99	79.76	1.000	0.095	58.34	55.28	61.54	61.38	0.99974
Apple	0.0017	76.37	73.16	79.74	79.85	1.000	0.096	58.32	55.24	61.49	61.50	0.99992
Sunflower	0.0013	76.96	73.68	80.39	80.72	1.000	0.085	58.84	55.75	62.00	62.05	0.99987
Rose	0.0017	76.25	73.06	79.73	79.55	1.000	0.097	58.27	55.16	61.49	61.49	0.99991
Grape	0.0013	76.38	73.19	79.70	79.85	1.000	0.096	58.30	55.22	61.46	61.49	0.99983
Tomato	0.0013	76.69	73.77	79.39	79.64	1.000	0.096	58.32	55.23	61.47	61.48	0.99960
Average	**0.0015**	**76.47**	**73.28**	**79.82**	**79.90**	**1.000**	**0.094**	**58.40**	**55.31**	**61.58**	**61.57**	**0.99981**

Table 4 presents the MSE, PSNR and SSIM values which are obtained by the LSB substitution two-bit used to hide the message 1 and message 2 into the cover images. The average MSE, PSNR and SSIM values for the message1 are calculated as 0.0015, 76.47 and 1 respectively, while it is computed as 0.094, 58.40 and 0.99981 for message 2.

Table 5 presents the MSE, PSNR and SSIM values which are obtained by the LSB substitution three-bit used to hide the message 1 and message 2 into the cover images. The average MSE, PSNR and SSIM values for the message1 are calculated as 0.0053, 70.79 and 0.99999 respectively, while it is computed as 0.339, 52.84 and 0.99949 for message 2.

Table 5. *LSB substitution three-bit performance analysis for message 1 and message 2*

Cover Image	**Embedded message 1 (3560 bits)**						**Embedded message 2 (245792 bits)**					
	MSE	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**	**MSE**	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**
Garlic	0.0053	70.74	69.24	69.73	75.60	0.999	0.349	52.70	51.46	51.40	57.68	0.99916
Apple	0.0057	70.68	69.34	69.57	75.23	0.999	0.345	52.75	51.37	51.59	57.68	0.99982
Sunflower	0.0050	71.25	70.02	69.99	76.05	0.999	0.305	53.29	51.87	52.20	58.14	0.99956
Rose	0.0057	70.55	69.04	69.52	75.52	0.999	0.332	52.93	51.69	51.67	57.67	0.99976
Grape	0.0053	70.79	69.71	69.37	75.63	0.999	0.344	52.77	51.37	51.64	57.68	0.99949
Tomato	0.0053	70.75	69.42	69.63	75.32	0.999	0.358	52.59	50.87	51.76	57.76	0.99917
Average	**0.0053**	**70.79**	**69.46**	**69.64**	**75.56**	**0.999**	**0.339**	**52.84**	**51.44**	**51.71**	**57.77**	**0.99949**

Table 6 presents the MSE, PSNR and SSIM values which are obtained by the PVD used to hide the message 1 and message 2 into the cover images. The average MSE, PSNR and SSIM values for the message1 are calculated as 0.0053, 71.58 and 0.999 respectively, while it is computed as 0.392, 52.52 and 0.9995 for message 2.

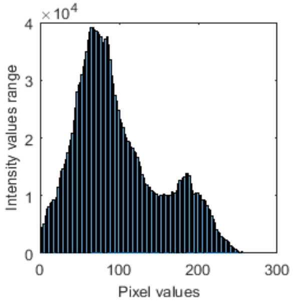
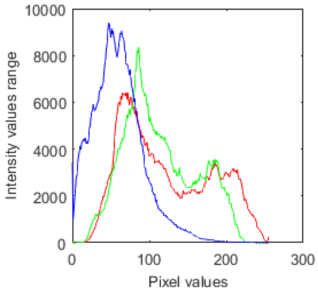
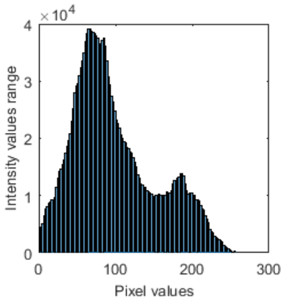
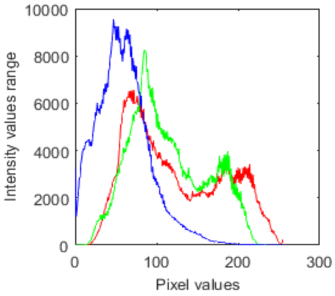
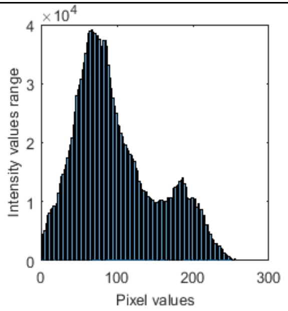
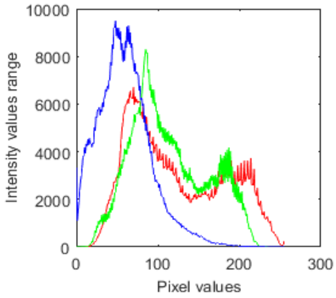
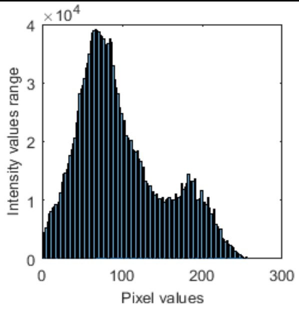
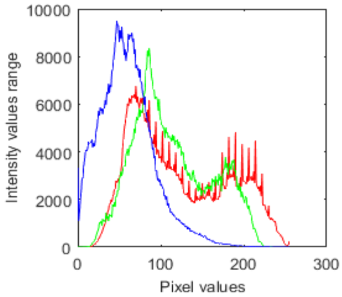
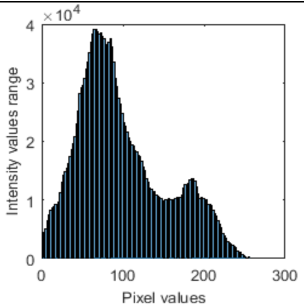
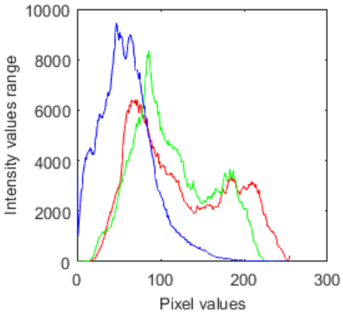
According to the data presented in Tables 3-6, the SSIM values for message 1 and message 2 are very close to 1, and the similarity between the cover image and the stego image is observed very high. When the PSNR values are examined, it was observed that the LSB substitution one-bit achieves a high PSNR compared to other used methods because of changing the last one bit. On the other hand, the agricultural data in the stego image are easy to detect by third parties, hence the security weakness is higher. PVD provides safe data hiding algorithm which is more difficult to be perceived and obtained data by the third party despite low PSNR value. When the results of the LSB methods presented in Tables 3-5 are examined, there is no difference between the MSE, PSNR and SSIM values obtained from different cover images in the same method. Table 6 shows that the MSE, PSNR and SSIM values are lower than the other cover images in the PVD method due to size and difference between color channels of the sunflower cover image.

Table 6. *PVD performance analysis for message 1 and message 2*

Cover Image	**Embedded message 1 (3560 bits)**						**Embedded message 2 (245792 bits)**					
	MSE	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**	**MSE**	**PSNR**	**PSNR Red**	**PSNR Green**	**PSNR Blue**	**SSIM**
Garlic	0.0040	72.13	71.86	72.14	72.42	0.999	0.341	52.81	52.77	52.66	53.00	0.99934
Apple	0.0040	72.26	72.32	72.39	72.07	0.999	0.276	53.73	53.51	53.59	54.10	0.99984
Sunflower	0.0143	66.57	66.17	66.83	66.76	0.999	0.753	49.36	49.11	49.24	49.76	0.99941
Rose	0.0027	73.73	73.48	73.95	73.77	1.000	0.414	51.96	52.08	51.86	51.95	0.99978
Grape	0.0037	72.36	72.57	72.15	72.37	0.999	0.321	53.07	53.17	53.13	52.91	0.99963
Tomato	0.0037	72.41	72.09	72.50	72.67	0.999	0.249	54.16	54.10	54.11	54.28	0.99898
Average	**0.0053**	**71.58**	**71.42**	**71.66**	**71.68**	**0.999**	**0.392**	**52.52**	**52.46**	**52.43**	**52.67**	**0.99950**

Table 7 shows a comparative performance analysis of LSB substitution one-bit, two-bit, three-bit and PVD methods for message 2 and the apples cover image. In the table, we present the cover image, the stego images, general and color channel-based histograms for used image steganography methods. While, in LSB based methods, the stego image histograms differ with the cover image histogram, it is difficult to perceive this difference almost human eye in the PVD method.

Table 7. *Performance analysis of used methods for message 2*

	Image	General histogram	Color based histogram
Cover			
LSB one-bit			
LSB two-bit			
LSB three-bit			
PVD			

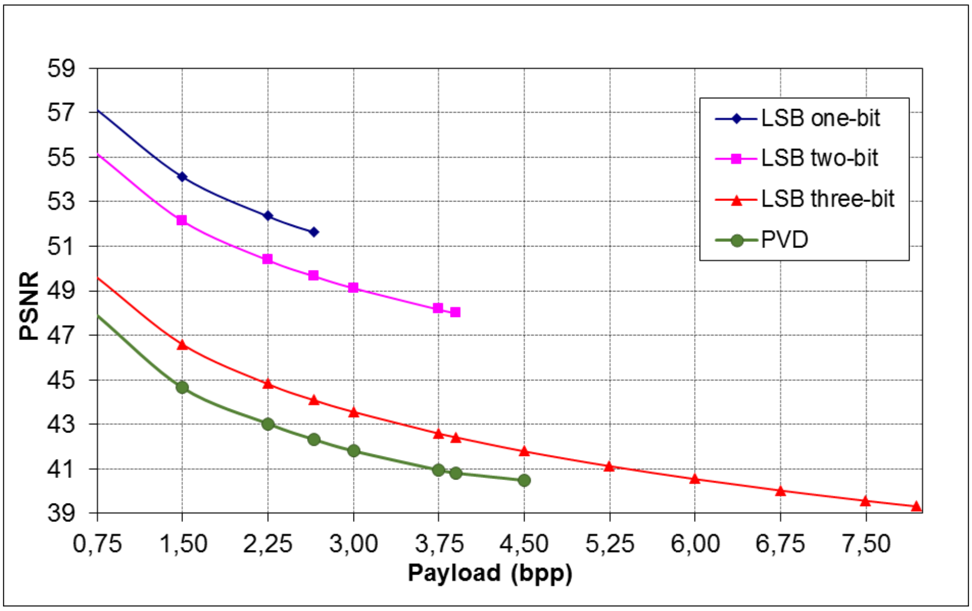


Figure 11*. A comparison of PSNR and payload values of the rose cover image for used algorithms*

Figure 11 shows a comparative performance analysis of PSNR and payload values for the rose cover image at four different algorithms applied in the study. In LSB substitution one-bit, the agricultural data between 500,000 and 1,778,666 bits are hidden in the cover image, and PSNR values are between 51.60 and 57.13. In LSB substitution two-bit, the agricultural data between 500,000 and 2,668,000 bits are hidden in the cover image, and PSNR values are between 47.95 and 55.15. In LSB substitution three-bit, the agricultural data between 500,000 and 5,336,000 bits are hidden in the cover image, and PSNR values are between 39.31 and 49.61. In the PVD method, the agricultural data between 500,000 and 3,203,320 bits are hidden in the cover image, and PSNR values are between 40.33 and 47.90. The highest PSNR value is obtained by LSB substitution one-bit method, and the highest payload value is obtained by LSB substitution three-bit.

5. CONCLUSIONS

In our paper, we propose an effective and secure image steganography-based GUI, which is designed to hide the agricultural data in the cover image and extract it from the stego image. After the agricultural data is encrypted with additional protection, which is the embedded key and shifting operations, it is hidden in the cover image with four different steganography method as LSB substitution one-bit, two-bit, three-bit and PVD. Even if it is detected that there is agricultural data within the stego image, this data cannot be accurately decrypted by third parties due to the additional security measures employed. The GUI hides agricultural data on agricultural cover image so that data can be securely stored in a single image file without the demand for another file or database. Besides the person who owns the agricultural image can hide their signature data in the image so that no one can notice it.

This is the first study in the field of agriculture, in which the agricultural data taken from the database are hidden by image steganography methods. The capacity and stego image quality are examined while comparing these methods in the prepared GUI. While the LSB substitution one-bit and two-bit can hide agricultural data with high PSNR values in the cover image, the LSB substitution three-bit produces low PSNR values but hides great amounts of data. The PVD can hide agricultural data in the cover image more securely than LSB substitution one-bit, two-bit and three-bit.

Further studies are necessary to improve the capacity of agricultural data to be placed in the cover image. Therefore, we will produce a hybrid method with high capacity and security, which will use LSB and PVD together.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Too, E. C., Yujian, L., Njuki, S., Yingchun, L., "A comparative study of fine-tuning deep learning models for plant disease identification ", Computers and Electronics in Agriculture, 161: 272-279, (2018**)**.

[2] Solak, S., Altinişik, U., "A new method for classifying nuts using image processing and k-means++ clustering", Journal of Food Process Engineering, 41(7): e12859, (2018).

[3] Huang, X. Y., Pan, S. H., Sun, Z. Y., Ye, W. T., Aheto, J. H., "Evaluating quality of tomato during storage using fusion information of computer vision and electronic nose ", Journal of Food Process Engineering, 41(6): e12832, (2018).

[4] Kruse, O. M. O., Prats-Montalbán, J. M., Indahl, U. G., Kvaal, K., Ferrer, A., Futsaether, C. M., "Pixel classification methods for identifying and quantifying leaf surface injury from digital images", Computers and Electronics in Agriculture, 108: 155-165, (2014).

[5] Vithu, P., Moses, J. A., "Machine vision system for food grain quality evaluation: A review", Trends in Food Science & Technology, 56: 13-20, (2016).

[6] Kumar, K., Kumar, S., Sankar, V., Sakthivel, T., Karunakaran, G., Tripathi, P. C., "Non-destructive estimation of leaf area of durian (Durio zibethinus)–An artificial neural network approach", Scientia Horticulturae, 219: 319-325, (2017).

[7] Aydoğan, T., Bayılmış, C., "A new efficient block matching data hiding method based on scanning order selection in medical images", Turkish Journal of Electrical Engineering & Computer Sciences, 25(1): 461-473, (2017).

[8] Ropodi, A. I., Panagou, E. Z., Nychas, G. J., "Data mining derived from food analyses using non-invasive/non-destructive analytical techniques; determination of food authenticity, quality & safety in tandem with computer science disciplines", Trends in Food Science & Technology, 50: 11-25, (2016).

[9] Rong, D., Ying, Y., Rao, X., "Embedded vision detection of defective orange by fast adaptive lightness correction algorithm", Computers and Electronics in Agriculture, 138: 48-59, (2017).

[10] Beyaz, A., Özkaya, M. T., İçen, D., "Identification of some spanish olive cultivars using image processing techniques", Scientia Horticulturae, 225: 286-292, (2017).

[11] Peng, Y., Zhang, L., Song, Z., Yan, J., Li, X., Li, Z., "A QR code based tracing method for fresh pork quality in cold chain", Journal of Food Process Engineering, 41(4): e12685, (2018).

[12] Kale, A. P., Sonavane, S. P., "IoT based Smart Farming: Feature subset selection for optimized high-dimensional data using improved GA based approach for ELM", Computers and Electronics in Agriculture, 161: 225-232, (2018).

[13] Colezea, M., Musat, G., Pop, F., Negru, C., Dumitrascu, A., Mocanu, M., "CLUeFARM: Integrated web-service platform for smart farms ", Computers and Electronics in Agriculture, 154: 134-154, (2018).

[14] Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., Nillaor, P., “IoT and agriculture data analysis for smart farm ”, Computers and Electronics in Agriculture, 156: 467-474, (2019).

[15] Kamilaris, A., Prenafeta-Boldú, F. X., “Deep learning in agriculture: A survey ”, Computers and Electronics in Agriculture, 147: 70-90, (2018).

[16] Diffie, W., Hellman, M., “New directions in cryptography ”, IEEE Transactions on Information Theory, 22(6): 644-654, (1976).

[17] Dhiman, K., Kasana, S. S., “Extended visual cryptography techniques for true color images ”, Computers & Electrical Engineering, 70: 647-658, (2018).

[18] Solak, S , Altınışık, U., “A new approach for steganography: Bit shifting operation of encrypted data in LSB (SED-LSB)”, Bilişim Teknolojileri Dergisi, 12(1): 75-81, (2019).

[19] Johnson, N. F., Jajodia, S., “Exploring steganography: Seeing the unseen”, Computer, 31(2): 26-34, (1998).

[20] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., Jung, K. H., “Image steganography in spatial domain: A survey ”, Signal Processing: Image Communication, 65: 46-66, (2018).

[21] Solak, S , Altınışık, U ., “The least significant two-bit substitution algorithm for image steganography ”, International Journal of Computer (IJC), 31(1): 150-156, (2018).

[22] Solak, S., Altınışık, U., “LSB substitution and PVD performance analysis for image steganography ”, International Journal of Computer Sciences and Engineering, 6(10): 1-4, (2018).

[23] Petitcolas, F. A., Anderson, R. J.,Kuhn, M. G., “Information hiding-a survey”, Proceedings of the IEEE, 87(7): 1062-1078, (1999).

[24] Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P., “Digital image steganography: Survey and analysis of current methods”, Signal Processing, 90(3): 727-752, (2010).

[25] Bender, W., Gruhl, D., Morimoto, N., Lu, A., “Techniques for data hiding ”, IBM Systems Journal, 35(3.4): 313-336, (1996).

[26] Solak, S., Altınışık, U., “Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3”, Journal of Electronic Imaging, 28(4): 043025, (2019).

[27] Walia, G. S., Makhija, S., Singh, K., Sharma, K., “Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map”, Optik, 170: 106-124, (2018).

[28] Ibanez, A. L., Djamal, E. C., Ilyas, R., Najmurrokhman, A., “Optimization of least significant bit steganography using genetic algorithm to improve data security”, In 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE). IEEE, 523-528, (2018).

[29] Shreelekshmi, R., Wilscy, M., Madhavan, C. V., “Undetectable least significant bit replacement steganography”, Multimedia Tools and Applications, 78(8): 10565-10582, (2019).

[30] Wu, D. C., Tsai, W. H., “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters, 24(9-10): 1613-1626, (2003).

[31] Wang, C. M., Wu, N. I., Tsai, C. S., Hwang, M. S., “A high quality steganographic method with pixel-value differencing and modulus function”, Journal of Systems and Software, 81(1): 150-158, (2008).

[32] Chen, J., “A PVD-based data hiding method with histogram preserving using pixel pair matching”, Signal Processing: Image Communication, 29(3): 375-384, (2014).

[33] Swain, G., “Adaptive pixel value differencing steganography using both vertical and horizontal edges ”, Multimedia Tools and Applications, 75(21): 13541-13556, (2016).

[34] Hussain, M., Wahab, A. W. A., Ho, A. T., Javed, N., Jung, K. H., “A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement ”, Signal Processing: Image Communication, 50: 44-57, (2017).

[35] Prasad, S., Pal, A. K., “An RGB colour image steganography scheme using overlapping block-based pixel-value differencing ”, Royal Society Open Science, 4(4): 161066, (2017).

[36] Li, Z., He, Y., “ Steganography with pixel-value differencing and modulus function based on PSO”, Journal of Information Security and Applications, 43: 47-52, (2018).

[37] Plants Database, “The National Gardening Association”, https://garden.org/plants/group/. Access date: February 2020.

[38] Turkomp, “Turkish Food Composition Database”, http://www.turkomp.gov.tr/main. Access date: February 2020.

[39] Eurofir, http://www.eurofir.org/food-information/food-composition-databases/. Access date: February 2020.

[40] Biringen Löker, G., Amoutzopoulos, B., Özge Özkoç, S., Özer, H., Şatir, G., Bakan, A., “A pilot study on food composition of five Turkish traditional foods.”, British Food Journal, 115(3): 394-408, (2013).

[41] Kocak, C., “Clsm: Couple layered security model a high-capacity data hiding scheme using with steganography ”, Image Analysis & Stereology, 36(1): 15-23, (2017).

[42] Jung, K. H., “Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane ”, Journal of Real-Time Image Processing, 14(1): 127-136, (2018).

[43] Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P., “Image quality assessment: from error visibility to structural similarity ”, IEEE Transactions on Image Processing, 13(4): 600-612, (2004).

[44] Konyar, M. Z., Öztürk, S., “Reed solomon coding-based medical image data hiding method against salt and pepper noise ”, Symmetry, 12(6): 899, (2020).

[45] Solak, S., “High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms ”, IEEE Access, 8: 166513-166524, (2020).