IRSTI 27.47.23 DOI: https://doi.org/10.26577/JMMCS2024121112

I. Saymanov
National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan, Tashkent
Engineering Federation of Uzbekistan, Uzbekistan, Tashkent
e-mail: islambeksaymanov@gmail.com

LOGICAL AUTOMATIC IMPLEMENTATION OF STEGANOGRAPHIC CODING ALGORITHMS

The main goal of steganography is to ensure secure communication while keeping the communicative act "invisible". The origin of this term dates back to Ancient Greece and translates as "hidden writing". A simple yet effective method of steganography in antiquity, considering the frequent use of wax tablets, involved cutting out the message on the wooden bottom of the tablet and then writing a decoy message on the wax. Technological evolution has led to human ingenuity, allowing the use of this powerful tool for both message transmission and watermarking products during the transition from physical to digital media. There are various forms of steganography, including injective, generative, substitutive, selective, and constructive. The steganography we employ is injective, as it is more suitable for our task of hiding information in image pixels. After various searches, we decided to use BMP (Bitmap Picture) 3 (Microsoft Windows NT) and later versions as the image file format, as this version, especially in 24-bit and 32-bit encodings, represents a single color component. Each byte allows for altering the least significant bits without changing the external appearance of the image.

Key words: logical automatic implementation, steganographic coding, algorithms, RGB (Red, Green, Blue), LSB (Least Significant Bit), PSNR (peak signal to-noise ratio).

И. Сайманов
Мирзо Улугбек атындағы Өзбекстан Ұлттық университеті, Өзбекстан, Ташкент қ.
Өзбекстанның инженерлік федерациясы, Өзбекстан, Ташкент қ.
e-mail: islambeksaymanov@gmail.com

Стеганографиялық кодтау алгоритмдерін логикалық автоматты жүзеге асыру

Стеганографияның негізгі мақсаты коммуникативті актіні "көрінбейтін"сақтай отырып, қауіпсіз байланысты қамтамасыз ету. Бұл терминнің шығу тегі Ежелгі Грециядан басталады және "жасырын жазу"деп аударылады. Ежелгі дәуірде балауыз таблеткаларын жиі қолдануды ескере отырып, стеганографияның қарапайым, бірақ тиімді әдісі планшеттің ағаш түбіндегі хабарламаны кесіп алуды, содан кейін балауызға алдау хабарламасын жазуды қамтиды. Технологиялық эволюция адамның тапқырлығына әкеліп соқты, бұл қуатты құралды физикалық медиадан цифрлық тасымалдағышқа көшу кезінде хабарларды жіберу үшін де, өнімдерді су таңбалау үшін де пайдалануға мүмкіндік берді. Стеганографияның инъекциялық, генеративті, алмастырушы, селективті және конструктивті сияқты әртүрлі формалары бар. Біз қолданатын стеганография инъекциялық болып табылады, өйткені ол кескін пикселдеріндегі ақпаратты жасыру міндетімізге қолайлырақ. Түрлі іздеулерден кейін біз BMP 3 (Microsoft Windows NT) және одан кейінгі нұсқаларын кескін файлының пішімі ретінде пайдалануды шештік, өйткені бұл нұсқа, әсіресе 24-биттік және 32-биттік кодтауларда, бір түсті құрамдас бөлікті білдіреді. Әрбір байт кескіннің сыртқы көрінісін өзгертпестен ең аз маңызды биттерді өзгертуге мүмкіндік береді.

Түйін сөздер: логикалық автоматты іске асыру, стеганографиялық кодтау, алгоритмдер, RGB (Қызыл, Жасыл, Көк), LSB (Ең аз маңызды бит), PSNR (сигналдың шуылға қатынасы шыңы).

И. Сайманов
Национальный университет Узбекистана имени Мирзо Улугбека, Узбекистан, г. Ташкент
Инженерная Федерация Узбекистана, Узбекистан, г. Ташкент
e-mail: islambeksaymanov@gmail.com

Логическая автоматная реализация алгоритмов стеганографического кодирования

Основная цель стеганографии обеспечить безопасную связь, сохраняя при этом коммуникативный акт "невидимым". Происхождение этого термина восходит к Древней Греции и переводится как "скрытое письмо". Простой, но эффективный метод стеганографии в древности, учитывая частое использование восковых табличек, заключался в вырезании сообщения на деревянном дне таблички, а затем написании ложного сообщения на воске. Технологическая эволюция привела к человеческой изобретательности, позволившей использовать этот мощный инструмент как для передачи сообщений, так и для нанесения водяных знаков на продукты при переходе от физических носителей к цифровым. Существуют различные формы стеганографии, включая инъективную, генеративную, замещающую, селективную и конструктивную. Используемая нами стеганография является инъективной, поскольку она больше подходит для нашей задачи по сокрытию информации в пикселях изображения. После различных поисков мы решили использовать в качестве формата файла изображения BMP 3 (Microsoft Windows NT) и более поздние версии, так как эта версия, особенно в 24-битной и 32-битной кодировке, представляет собой единую цветовую составляющую. Каждый байт позволяет изменять младшие биты без изменения внешнего вида изображения.

Ключевые слова: логическая автоматическая реализация, стеганографическое кодирование, алгоритмы, RGB (красный, зеленый, синий), LSB (младший значащий бит), PSNR (пиковое отношение сигнал/шум).

1 Introduction

The ability to utilize Arduino and any components that can be implemented sparked our interest in creating a useful and intriguing project for our participants [1]. Initially, the idea was to create a universal remote control panel that could be used in electronic equipment by using an infrared remote control to manage ecological process automation. After discussing other ideas, it was concluded that injective steganography could be an excellent tool to achieve the goal [2–8].

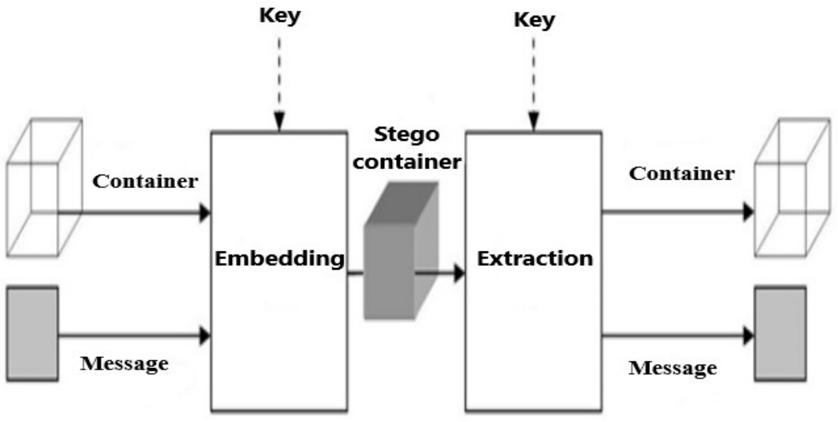


Figure 1: Generalized model of a steganographic system

The main goal of steganography is to ensure secure communication while keeping the communicative act "invisible". The origin of this term dates back to Ancient Greece and translates as "hidden writing". A simple yet effective method of steganography in antiquity, considering the frequent use of wax tablets, involved cutting out the message on the wooden bottom of the tablet and then writing a decoy message on the wax [9–14]. Technological evolution has led to human ingenuity, allowing the use of this powerful tool for both message transmission and watermarking products during the transition from physical to digital media [15–17]. There are various forms of steganography, including injective, generative, substitutive, selective, and constructive. The steganography we employ is injective, as it is more suitable for our task of hiding information in image pixels [18–24]. After various searches, we decided to use BMP 3 (Microsoft Windows NT) and later versions as the image file format, as this version, especially in 24-bit and 32-bit encodings, represents a single color component. Each byte allows for altering the least significant bits without changing the external appearance of the image. Therefore, supported raster images are 24-bit and 32-bit, because altering 8, 4, or 1 bit would be noticeable.

BMP format is one of the simplest formats jointly developed by Microsoft and IBM. A raster image file records the image as a table of points (pixels). It manages colors both in RGB (Red Green Blue) and through an indexed palette.

Our developed steganographer, as mentioned earlier, is compatible with both 32-bit and 24-bit raster image formats because we decided to use 4 image bytes to hide 1 byte of text. Of these 4 bytes, the first three are modified, and the last one should remain unchanged.

In the case of the 32-bit format (where R represents the red byte, G represents the green byte, B represents the blue byte), the least significant bit of the bytes will be modified in RGB.

The research provided systematic activities for image steganography, including hiding/embedding secret messages, revealing messages, as well as a systematic step-by-step approach to ensuring the execution of these steps. The research begins with explaining the new system, thereby giving a hint about its contents [25–29].

The proposed system employs a robust approach, involving embedding a secret message into one of the three RGB image color channels, bitwise processing, bit shuffling, a secret key, and cryptography to develop a new algorithm for steganography system. The new algorithm will provide the following important aspects of data security enhancement. Before matching the secret message to the image carrier by means of transposition, the intruder is misled.

The encryption of the secret key and data is encrypted using a reliable repetitive algorithm to ensure secure protection that cannot be easily cracked or broken.

The secret data will be hidden by matching them with the blue color frequency in the carrier image using a modification method for gray color.

Enhance file security on the Internet through efficient encryption and embedding of a secret message that can only be revealed by authorized third parties.

To ensure effective hiding of the secret message on the selected cover image, a different encryption method will be used. These modules include file matching and encryption methods to hide the secret message and ensure its security. A general diagram explaining the new methodology is presented in Figure 2 below.

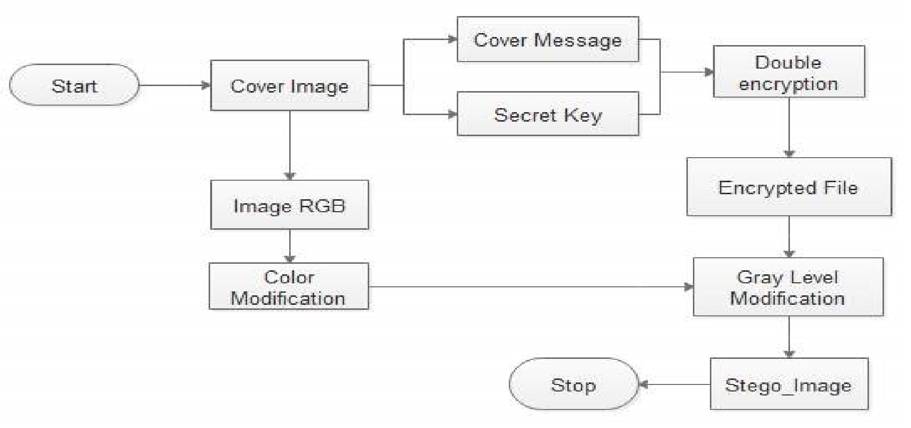


Figure 2: Steps of Text Concealment and Display on Image

2 Encryption Algorithm

This is a step-by-step approach used for concealing a message within an innocent image. This algorithm represents a procedural methodology developed to protect against malicious attacks on files over the Internet. The encryption algorithm is employed for concealment in this algorithm, precisely providing the first step in ensuring file security on the Internet, as well as serving as the first stage of image steganography adopted for this research. The algorithm begins by taking input about image concealment and outputs an encrypted stego-image with secret data and key bits. The encryption algorithm schema is presented below.

Inputs: original color image and document.

Output: Stego_Image consisting of a secret message.

Step 1: Select what needs to be concealed and the required encryption key.

Step 2: Convert the selected key into a one-dimensional array (1D array).

Step 3: Use logic 1 to apply the bitxor process to one bit of the secret key array with logical 1.

Step 4: Rearrange the encrypted bits from bitxor by swapping even and odd bits from step 2.

Logic: If the secret key bit = 1, perform the bitxor process with logical 1. Otherwise, do not implement the bitxor process.

Step 5: Repeat step 4 until all secret data bits are encrypted.

3 Cartographic module

The mapping procedure has been adopted for efficiently placing a secret message into a pixel of the carrier/cover image for final encryption. The cover image channels are transformed, followed by a 1-to-1 mapping to place the secret data into the cover image, preserving the bits and pixels of the original cover image to obtain the output steganographic image.

Input: cover image, secret message

Output: Stego_Image Step 1: Choose the carrier image.

Step 2: Transform the cover image from step 1.

Step 3: Select the secret file.

Step 4: Perform a 1-to-1 mapping to conceal the message from step 3 into the image from step 2.

Step 5: Stego image.

Concealment Algorithm.

Input: color image as cover, secret data, and key.

Output: Stego_image

Step 1: Choose the cover color image and divide it into red, green, and blue channels.

Step 2: Apply image transposition to all three channels of the input image.

Step 3: Encrypt the secret key and secret data according to encryption module 3.1.

Step 4: Transform pixel values for the blue channel by adding 1 if the first bit of the cover image equals one (1). If the pixel value is even, add one to the pixel.

Step 5: Map secret data from step 4 based on secret key bits (SKB) as follows: If secret key bits are even, the system adds one (1) to the pixel value. If pixel value equals the secret key bit value of 0 or is odd, subtract 1 from the pixel value. If pixel value of the secret bit equals 1 or is even, the system adds 1 to the pixel value.

Step 6: Repeat step 5 until all secret bits are mapped to gray levels of the carrier image.

Step 7: Transpose all three planes and combine them to make the steganographic image.

Convert the decoding algorithm of the LSB method to algebraic form as follows:

$Y_0 = Y_1 = 1;$ $Y_6 = \overline{X_1X_3};$ $Y_{11} = \overline{X_1X_3X_4}X_6\overline{X_7X_8};$

$Y_2 = X_1X_2;$ $Y_7 = \overline{X_1X_3}X_4X_5;$ $Y_{12} = \overline{X_2X_3X_5}X_6\overline{X_7X_8};$

$Y_3 = \overline{X_1};$ $Y_8 = \overline{X_1X_3X_4};$ $Y_{13} = \overline{X_1X_3X_4X_6}X_9;$

$Y_4 = \overline{X_1};$ $Y_9 = \overline{X_1X_3X_4}X_6X_7;$ $Y_{14} = \overline{X_1X_3X_4X_6X_9};$

$Y_5 = \overline{X_1}X_3;$ $Y_{10} = \overline{X_1X_3X_4}X_6\overline{X_7}X_8;$ $Y_k = \overline{X_1X_3X_4}X_5\overline{X_6}\vee; \overline{X_1X_3}X_4\overline{X_5}$

Unfortunately, it seems like the matrix scheme you mentioned is not provided in the text you provided. If you have the matrix scheme or any specific details you'd like to discuss or analyze regarding the LSB (Least Significant Bit) encoding and decoding algorithm, please feel free to provide them, and I'd be happy to assist you further.

$Y_0 = Y_1;$ $Y_8 = Y_9;$

$Y_1 = X_1X_2Y_2 \vee \overline{X_1}Y_3;$ $Y_9 = X_5Y_{10} \vee \overline{X_5}X_6X_7Y_{11} \vee \overline{X_5}X_6\overline{X_7}Y_{12} \vee \overline{X_5X_6};$

$Y_2 = X_1X_2Y_2 \vee \overline{X_1}Y_3;$ $Y_{10} = Y_9;$

$Y_3 = Y_4;$ $Y_{11} = Y_{13};$

$Y_4 = X_3Y_5 \vee \overline{X_3}Y_6;$ $Y_{12} = Y_{13};$

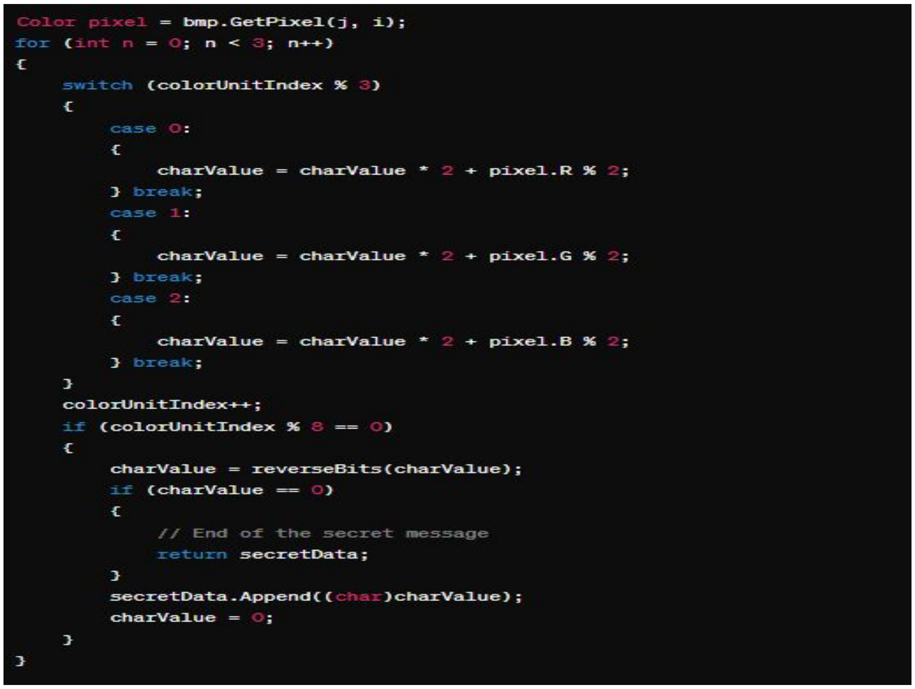
$Y_5 = Y_4;$ $Y_{13} = X_6X_7\overline{X_8}Y_{11} \vee X_6\overline{X_7X_8}Y_{12} \vee X_8Y_{14} \vee \overline{X_6X_8}Y_{15};$

$Y_6 = X_4Y_7 \vee \overline{X_4}Y_8;$ $Y_{14} = \overline{X_6}Y_{15};$

$Y_7 = X_4Y_7 \vee \overline{X_4}Y_8;$ $Y_{15} = Y_k;$

4 Extracting Algorithm.

The extraction algorithm delineates the sequential steps outlined in a flowchart aimed at extracting text from an image. The user is required to input both the key file and the steganographic image generated earlier. It is imperative that the same key file is employed during both the hiding and extraction phases. Subsequently, upon user input, the provided data undergoes scrutiny and validation for any potential exceptions. In the event of exception detection, the process iterates from the beginning. Conversely, if no exceptions are encountered, the algorithm proceeds with the extraction process by implementing modifications to retrieve the secret message from the image file. This extracted secret message is then displayed on the screen or saved in a file.



```
Color pixel = bmp.GetPixel(j, i);
for (int n = 0; n < 3; n++)
{
    switch (colorUnitIndex % 3)
    {
        case 0:
        {
            charValue = charValue * 2 + pixel.R % 2;
        } break;
        case 1:
        {
            charValue = charValue * 2 + pixel.G % 2;
        } break;
        case 2:
        {
            charValue = charValue * 2 + pixel.B % 2;
        } break;
    }
    colorUnitIndex++;
    if (colorUnitIndex % 8 == 0)
    {
        charValue = reverseBits(charValue);
        if (charValue == 0)
        {
            // End of the secret message
            return secretData;
        }
        secretData.Append((char)charValue);
        charValue = 0;
    }
}
```

Figure 3: Extract the least significant bit of the blue channel.

5 Assessment of picture quality

This aspect involves examining the original image and the developed stego_image to determine whether any detectable changes or physical modifications to the original image will occur, thus verifying the effectiveness of the algorithms and steps taken in developing steganography. The quality of each (i.e., the original image and the resulting steganographic file) is carefully analyzed using common measures used for comparing the degree of quality.

The new steganographic algorithm has a high embedding capacity and low visual distortion. Encryption methods are resistant to malicious attacks, including adding noise, smoothing, quantization, and ordinary grid editing. Besides reliability, the new algorithm provides acceptable embedding capacity without noticeable visual distortion after embedding.

The efficacy of the novel encryption and steganography techniques is assessed in relation to their embedding capacity, embedding distortion, and reliability. The discrepancy in embedding distortion between the initial grid and its corresponding counterpart is scrutinized through metrics such as the root mean square error (RMSE), peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), and extracted reliability.

Mean Squared Error (MSE) is employed as a measure of similarity between images, elucidating the degree of distortion between the original and Stego_image. It serves as a signal image quality metric, extensively utilized for assessing image quality due to its simplicity in determination, effectiveness in gauging image optimization, and ease of parameter calculation.

$$MSE = \tfrac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$

The computation of the Mean Squared Error (MSE) between two images adheres to the aforementioned equation, wherein M and N represent the number of rows and columns of the cover image, respectively. Y and X denote the signals of the Stego image and the original image, respectively.

It is imperative to note that the Mean Squared Error is significantly influenced by the intensity scaling of the image. For instance, an MSE value of 100.0 achieved in an 8-bit image context (with pixel values ranging from 0 to 255) is deemed satisfactory. Conversely, an MSE value of 100.0 attained in a 10-bit image context (with pixel values ranging from 0 to 1023) is scarcely discernible and lacks substantial significance.

The Peak Signal-to-Noise Ratio (PSNR) provides an explanation of image quality by offering the ratio of the image signal to the power of image distortion in a logarithmic scale. It is also considered as a relative explanation of human perception of image quality. The higher the PSNR, the higher the image quality.

The PSNR is calculated by scaling the Mean Squared Error according to the image range.

$$PSNR = 10 \log \left[\tfrac{255^2}{MSE} \right]$$

Peak Signal-to-Noise Ratio (PSNR) values are conventionally expressed in decibels (dB). PSNR serves as a robust measure for comparing the outcomes of recovering identical images from various manipulations or compression processes. However, it's important to note that comparing PSNR values between different images holds lesser significance due to factors such as image content, resolution, and compression artifacts, which can significantly influence the perceived quality of the images. Therefore, while PSNR is valuable for assessing the fidelity of image recovery within the same context, its utility diminishes when used for comparing the quality of distinct images.

Signal-to-Noise Ratio (SNR) provides the ratio of signal power to noise power. It is an index that indicates the level of changes and influence on images based on a specific effect (such as steganography), providing a measure of the quantity/level of image transformation.

SNR is expressed in the formula below:

$$SNR = 10\text{log}_{10} \tfrac{signal}{noise}$$

Normalized Cross-Correlation (NCC) compares two images based on their common relationships. It is used to measure how two images deviate from or relate to each other. NCC is expressed in the formula below:

$$NCC = \frac{\sum\limits_{x=1}^{M} \sum\limits_{y=1}^{N} (S(x,y) \cdot C(x,y))}{\sum\limits_{x=1}^{M} \sum\limits_{y=1}^{N} (S(x,y))}$$

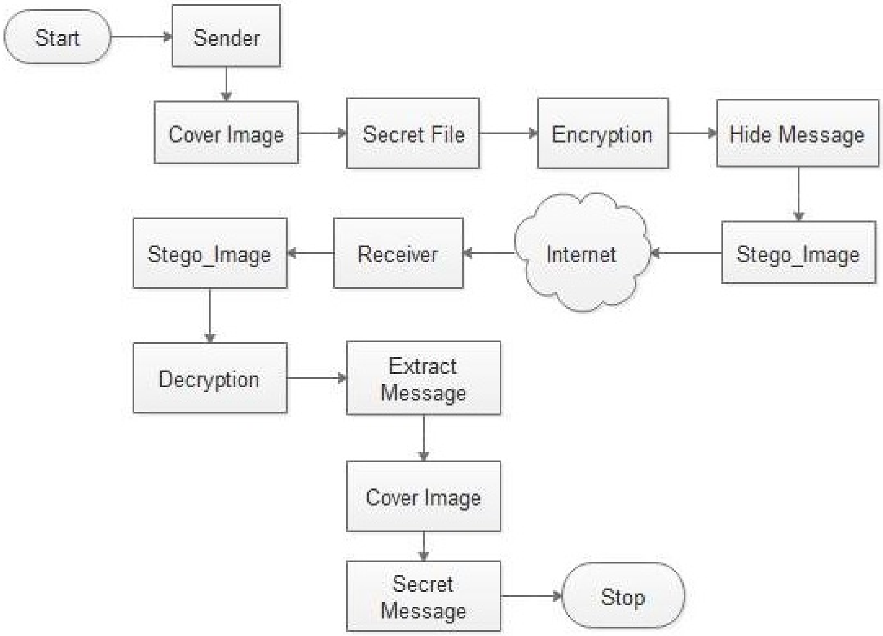


Figure 4: Extract the least significant bit of the blue channel.

The user is required to upload an image file, then select the level of security. The transmitted message is entered into the message field, after which the user enters their password for encrypting and embedding the secret message into the image (see Figure 4).

Finally, the user clicks the "Write Message to Image"button. After the appropriate measures have been taken, the user will need to upload a new image containing the secret message, i.e., the "Crypto-Stego Image". The algorithm used for the LSB method greatly complicates the detection of changes in images sent and received over the Internet by the human eye.

6 Conclusion

A logical method of steganographic encoding has been developed for the secure storage and transmission of images based on Boolean functions in the class of disjunctive normal forms using microcontrollers and CAD systems for designing programmable logic controllers. Methods and algorithms of steganographic encoding have been developed and implemented for the secure storage and transmission of images in an ecological system based on IoT technologies.

References

[1] Kabulov A., Saymanov I., Yarashov I. and Muxammadiev F., "Algorithmic method of security of the Internet of Things based on steganographic coding *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2021): 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

[2] Kabulov A., Normatov I., Urunbaev E., Muhammadiev F., "Invariant Continuation of Discrete Multi-Valued Functions and Their Implementation *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2021): 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422486.

[3] Kabulov A., Normatov I., Seytov A., Kudaybergenov A., "Optimal Management of Water Resources in Large Main Canals with Cascade Pumping Stations *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2020: 1-4, doi: 10.1109/IEMTRONICS51293.2020.9216402.

[4] Kabulov, A. V., Normatov, I. H., "About problems of decoding and searching for the maximum upper zero of discrete monotone functions *Journal of Physics: Conference Series*, 1260(10), 102006, 2019. doi:10.1088/1742-6596/1260/10/102006.

[5] Kabulov, A. V., Normatov, I. H., Ashurov A.O., "Computational methods of minimization of multiple functions *Journal of Physics: Conference Series*, 1260(10), 10200, 2019. doi:10.1088/1742-6596/1260/10/102007.

[6] SaвЂ™ed Abed, Al-Mutairi Mohammed, Al-Watyan Abdullah, Al-Mutairi Omar, AlEnizy Wesam, Al-Noori Aisha, "An Automated Security Approach of Video Steganography–Based LSB Using FPGA Implementation"*Journal of Circuits, Systems and Computers*, Vol. 28, no. 05, (2019): 1950083.

[7] Abdulrahman Abdullah Alghamdi, "Computerized Steganographic Technique Using Fuzzy Logic"*International Journal of Advanced Computer Science and Applications*, Vol. 9, no. 3, (2018): 155-159.

[8] Bruno Carpentieri, Castiglione Arcangelo, De Santis Alfredo, Palmieri Francesco, Pizzolante Raffaele, "Compression-Based Steganography"*Concurrency and Computation: Practice and Experience*, Vol. 32, no. 8, (2020).

[9] Mathivanan P., et al., "QR Code Based Color Image Stego-Crypto Technique Using Dynamic Bit Replacement and Logistic Map"*Optik*, Vol. 225, (2021): 1-24.

[10] Gurunath R., Alahmadi Ahmed H., Debabrata Samanta, Mohammad Zubair Khan, Abdulrahman Alahmadi, "A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks"*IEEE Access*, Vol. 9 (2021): 120869вЂ“120879.

[11] MegГas David, Wojciech Mazurczyk, Minoru Kuribayashi, "Data Hiding and Its Applications: Digital Watermarking and Steganography"*Applied Sciences*, (2021): 1вЂ“7.

[12] Kabulov A., Yarashov I., Otakhonov A., "Algorithmic Analysis of the System Based on the Functioning Table and Information Security *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2022): 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.

[13] Kabulov A., Saymanov I., Yarashov I., Karimov A., "Using Algorithmic Modeling to Control User Access Based on Functioning Table *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2022): 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850.

[14] Navruzov E., Kabulov A., "Detection and analysis types of DDoS attack *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2022): 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[15] Wenhao Chen, Lin Li, Newman Jennifer, Guan Yong, "Automatic Detection of Android Steganography Apps via Symbolic Execution and Tree Matching"*In 2021 IEEE Conference on Communications and Network Security (CNS)*, (2021): 254вЂ“262.

[16] Chiung-Wei Huang, Chou Changmin, Chiu Yu-Che, Chang Cheng-Yuan, et al., "Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography"*Mathematical Problems in Engineering*, (2018): 1-8.

[17] Lili Tang, Xie Jialiang, Wu Dongrui, "An Interval Type-2 Fuzzy Edge Detection and Matrix Coding Approach for Color Image Adaptive Steganography"*Multimedia Tools and Applications*, Vol. 81, no. 27, (2022): 39145вЂ“39167.

[18] Merve Varol Arsoy, "LZW-CIE: A High-Capacity Linguistic Steganography Based on LZW Char Index Encoding"*Neural Computing and Applications*, Vol. 34, no. 21, (2022): 19117 19145.

[19] Hala Salih Yusuf, Hani Hagras, "Towards Image Steganography Using Type-2 Fuzzy Logic and Edge Detection *In 2018 10th Computer Science and Electronic Engineering (CEEC)*, (2018): 75-78.

[20] Mukherjee Nabanita Goutam Paul, Sanjoy Kumar Saha, "An Efficient Multi-Bit Steganography Algorithm in Spatial Domain with Two-Layer Security *Multimedia Tools and Applications*, Vol. 77, (2018): 18451-18481.

[21] Xiang Lingyun, Rong Wang, Zhongliang Yang, Yuling Liu, "Generative Linguistic Steganography: A Comprehensive Review *KSII Transactions on Internet and Information Systems*, Vol. 16, no. 3, (2022): 986-1005.

[22] Zhongliang Yang, Zhang Pengyu, Jiang Minyu, Huang Yongfeng, Zhang Yu-Jin, "Rits: Real-Time Interactive Text Steganography Based on Automatic Dialogue Model *In International Conference on Cloud Computing and Security*, (2018): 253-264.

[23] Roseline Oluwaseun Ogundokun, Oluwakemi Christiana Abikoye, "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography *International Journal of Digital Multimedia Broadcasting*, (2021): 1-8.

[24] Tibor Gabor Attila, Jozsef Katona, "Development of Multi-Platform Steganographic Software Based on Random-LSB *Programming and Computer Software*, Vol. 49, no. 8, (2023): 922-941.

[25] Jayapandiyan Jagan Raj, Kavitha C., Sakthivel K., "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization *IEEE Access*, (2020): 136537-136545.

[26] Sathish Shet K., Aswath A.R., Hanumantharaju M.C., Gao Xiao-Zhi, "Novel High-Speed Reconfigurable FPGA Architectures for EMD-Based Image Steganography *Multimedia Tools and Applications*, Vol. 78, no. 13, (2019): 18309-18338.

[27] Iluminada Baturone, Barriga Angel, Jimenez-Fernandez Carlos, Lopez Diego R., Sanchez-Solano Santiago, "Microelectronic Design of Fuzzy Logic-Based Systems *CRC press*, (2018): 338.

[28] Safdar Munir M., Bajwa Imran Sarwar, Cheema Sehrish Munawar, "An Intelligent and Secure Smart Watering System Using Fuzzy Logic and Blockchain *Computers and Electrical Engineering*, Vol. 77, (2019): 109-119.

[29] Khan Muhammad, Jamil Ahmad, Muhammad Sajjad, Muhammad Zubair, "Secure Image Steganography using Cryptography and Image Transposition arXiv:1510.04413.