TEXNİKA ELMLƏRİ

UOT 025.3/.4:(084+086): 002.6:004.3

A NEW METHOD FOR HIDING CONFIDENTIAL INFORMATION IN COLOR IMAGES

Ababil Naghiyeva
Azerbaijan Technological University
ababil.nagiyeva@mail.ru
https://orcid.org/0000-0003-3071-1105

DOI: 10.30546/2958-8111.2025.2.9

Abstract

In this paper, a new method for embedding secret information into colored images is proposed and developed. The primary objectives of this method are to ensure its robustness, maintain the visual quality of the image, and allow for the embedding of a larger volume of secret information without noticeable degradation. To achieve these goals, the method employs the Scale-Invariant Feature Transform (SIFT) technique, which is used to address the robustness issue. SIFT helps ensure that the method can effectively withstand various image transformations, such as scaling, rotation, and changes in lighting conditions.

While SIFT provides strong robustness against geometric and photometric transformations, its public nature also poses a potential vulnerability. Since the algorithm and its outputs are widely known, adversaries can leverage the same technique to identify embedding regions, reducing the search area for steganalysis. To address this limitation, future approaches can enhance security by incorporating randomized keypoint perturbation, secret-key-based selection methods, or combining SIFT with other transformation-resistant embedding strategies.

By leveraging this approach, the method not only guarantees the preservation of key image features but also facilitates the secure embedding of secret data, thus improving the overall efficiency of steganographic processes in colored images.

Keywords: digital steganography, SIFT, image steganography, data hiding, secret information

Introduction

Today, the majority of multimedia content circulating on global computer networks and social media consists of colored, digital images. The use of colored images in this field is still in its developmental stages. It is also important to note that the application of colored images in steganography holds significant potential.

The structure of colored images allows for the embedding of a larger volume of secret information, while simultaneously ensuring the preservation of visual quality. When studying algorithms for hiding secret information in colored images, it becomes evident that the issue of robustness has not been sufficiently explored.

In colored images, keypoint pixels and their descriptors can be identified using the SIFT (Scale-Invariant Feature Transform) method. To ensure invariance, the following transformations are employed. Let us take a closer look at these transformations.

- Rotations
- Scaling (the same object may appear at different sizes in different images)
- Changes in brightness
- Changes in the camera's position (orientation).

To identify or detect keypoints, the Gaussian transform and Difference of Gaussians are used.

Although previous methods have used various color channels, the blue channel is selected in this research due to its low visibility to the human eye. Studies in visual perception show that the human eye is less sensitive to intensity changes in the blue spectrum [20, p.56-70]. This makes the blue channel a preferable option for embedding data that must remain imperceptible. Moreover, statistical steganalysis tools detect anomalies less effectively in the blue channel.

Research indicates that the human eye can perceive color values in the range of 400 nm (nanometers) to 700 nm. The color blue, however, falls between 400 nm and 500 nm, which is the first segment of the visible spectrum. Therefore, compared to other colors, blue is the least noticeable when changes are made. If the blue channel is used to hide secret information bits, it becomes significantly harder for malicious parties to detect the secret data (Figure 1).

In addition, recent works by Azerbaijani researchers have contributed to the development of secure steganographic techniques. For example, studies have explored the use of covert channels in applications like WhatsApp through graphic file formats and steganographic software developed for Windows and Android platforms [15, p.32-35]. Other research has proposed an improved method, such as a modified Least Significant Bit (LSB) technique using two graphic files to enhance reliability [6, p.1-10]. Such contributions play a crucial role in forming a localized research context.

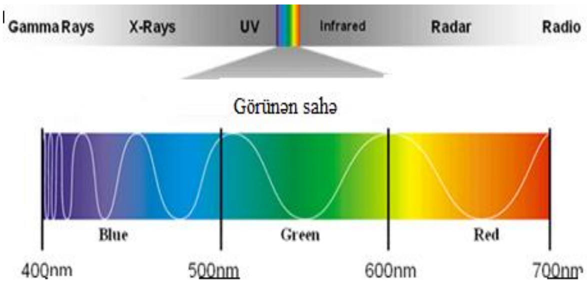


Fig 1. Electromagnetic Spectrum

In Figure 1, three color schemes and gamma rays, X-rays, ultraviolet rays, infrared rays, radar, and radio waves are shown. The figure demonstrates that the blue color channel indeed falls within the 400 nm to 500 nm range. Based on this, our goal is to embed secret information bits within this channel.

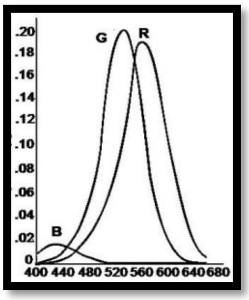


Fig. 2. Graph of the RGB Color Scheme

In the proposed secret information embedding algorithm, the secret information bits are hidden in the blue channel of the container image, specifically in the pixels selected by the SIFT algorithm. The SIFT algorithm is used to identify keypoint features in the image [5, p.130-134]. The SIFT algorithm also provides features that can be used for tasks such as object or scene recognition, 3D structure modeling, motion tracking, and comparison between images. Furthermore, it detects and extracts local features from images. Features extracted using the SIFT method are invariant to rotation, scaling, and illumination, making it useful for tasks such as scene modeling, recognition, and tracking [13, p.1-19].

Related work

In recent years, a large portion of the global population has been communicating with each other through e-mail, social networks, etc. The majority of these communications are accompanied by images. This, in turn, leads to the rapid development and corresponding use of image steganography. Recently, more well-known and widely spread steganographic methods are characterized by newly developed techniques. Image steganography is a modern field of information technology science that ensures the hiding of secret information within digital images (17, p.98-104, 8, p.3236-3246, 2019, 16, p. 647-654). Due to its advantages, image steganography has become more widespread compared to other methods. In image steganography, the process of embedding information involves using digital images as containers, which also act as carriers of the hidden information. The container must be chosen very carefully, as the effectiveness of the stego-system directly depends on the characteristics of the image [1, p.727-752]. Special methods for using digital images as containers have been developed [3, p.42-51, 9, p.94-103]

For this purpose, various statistical characteristics of images are compared, and samples are selected to ensure higher quality of the stego-image, the embedding of larger volumes of secret information, better visual quality indicators, and higher robustness. If a third party (attacker) has no knowledge of the transmitted information and does not suspect the existence of the hidden information, the communication system can be considered of high quality. Additionally, various technologies for improving the quality of containers have been developed and are used. One of these is the interpolation method for images.

Image steganography, after embedding the information into a digital image, results in the conversion of the image into a stego-image. The stego-image is then transmitted via an open communication channel to reach its destination. Information hiding algorithms may involve either the recovery or corruption of the container. In the first case, depending on the type of algorithm used, the secret information is extracted from the stego-image using either a stego-key or without one, and the container image returns to its original state. In the case of corruption, when the secret information is extracted from the stego-image, the container image becomes corrupted, i.e., it becomes unusable. Algorithms that allow for the recovery of the container are widely used [2, p.1-24, 11, p.102-112, 12, p.499-511, 21, p.553-562]

If the extraction of confidential information is not required in steganographic systems, such systems are considered blind stegosystems. The attack phase is carried out by a malicious actor when an anomaly is detected in the communication channel. The objectives of the adversary can vary in nature.

Attackers can be classified as either passive or active. The aim of a passive attacker is to detect the presence of hidden confidential information within the transmitted file. In contrast, an active attacker seeks to decrypt, disrupt, or damage the concealed information. A considerable number of scientific articles have been published in foreign literature concerning steganography.

Among these, a comprehensive review dedicated to steganography was prepared by Abbas Cheddad et al. [1, p.727-752], in which algorithms and methods related to digital images were extensively discussed.

In another work by Mehdi Huseyn et al., a broad overview of steganographic algorithms within the domain of spatial techniques in recent years was provided. The fundamental differences between cryptography, steganography, and watermarking were examined, and the architecture of steganographic systems based on various container formats was presented. A comparison of existing hiding algorithms was illustrated, highlighting their respective advantages and limitations. Furthermore, commonly used steganographic performance metrics, including steganalysis attacks, were discussed.

An overview of widely used digital image-based steganographic methods is provided in [1, p.727-752], and important formats using two categories of significant images are discussed. In many cases, before embedding secret information in image steganography, the cover image is processed using certain methods. One such method, widely used recently, is the Scale Invariant Feature Transform (SIFT) algorithm.

Proposed approach

In the proposed algorithm, the secret information bits are hidden in the pixels of the blue (B) channel of the RGB (Red, Green, Blue) color scheme container image by identifying key points using the SIFT algorithm. The secret information bits are then embedded at the identified key points. The randomness of embedding the secret information bits enhances the visual and security quality of the algorithm.

Confidential information bits are considered secure from a security perspective because they are hidden not in any arbitrary pixel or consecutive selected pixels in the blue channel of the color image, but in key point pixels determined by the SIFT algorithm. When hiding confidential information bits in the container image's specific pixels, it is intended that the information be converted into an octal number system before being embedded in the container image. This is because if confidential information bits are selected based on the octal number system, we would be embedding more confidential information bits compared to hiding them using binary number system-based algorithms. In the proposed algorithm, the sequence in which confidential information bits are embedded into the key point pixels determined by the SIFT algorithm is as follows.

Step 1: Key point pixels are detected using the SIFT algorithm.

Step 2: Among the identified key point pixels, those located in the blue channel are selected.

Step 3: Since the secret information bits are intended to be embedded in octal (base-8) form, the remainder obtained by dividing the pixels—determined according to formula (1) of the proposed algorithm—by eight is calculated.

$$n = p_{i,j} \bmod 8 \qquad (1)$$

Here, $p_{i,j}$ the pixel refers to that of the container image.

Step 4: The remainder value n obtained in Step 3 is converted into binary form.

$$n_{10} \to n'_2 .$$

Step 5: A number of secret information bits equal to the total number of ones and zeros in the obtained binary sequence are selected.

Step 6: The selected secret information bits are converted into the octal number system.

$$n_2 \to d_8$$

Step 7: In accordance with Equation (2), the obtained value is added to the pixel of the container image.

$$S_{ij} = p_{i,j} + d_8 \qquad (2)$$

Here, S_{ij} denotes the stego-image pixel, and $d_8$represents the secret information bit converted into the octal number system. Thus, the secret information bits are embedded into the container image.

Extraction of Secret Information Bits from the Stego-Image

To extract the secret information bits from the stegoimage, the following steps are performed in sequence:

Step 1: The receiver re-applies the SIFT algorithm to detect key points in the container image.

Step 2: The key point pixels that fall within the blue channel are identified.

Step 3: The SIFT algorithm is then applied to the stego-image to detect its key points.

Step 4: The corresponding pixels located in the blue channel are identified.

Step 5: The key point pixels identified in the blue channel of the container image are subtracted from those identified in the blue channel of the stegoimage, in accordance with equation (3).

$$M = S(i,j) - P(i,j) \qquad (3)$$

Here, M denotes the secret information bits, $S(i,j)$represents a specific pixel from the stegoimage, and $P(i,j)$ corresponds to the same pixel from the container image.

Step 6: The values obtained from the difference between $S(i,j)$ and $P(i,j)$ are converted into binary form, and the resulting bit sequences are concatenated. Thus, the secret information bits are successfully retrieved.

Experimental results

To ensure the accuracy of the experiments, the color standard images used in the compared algorithms were examined. In this algorithm, the secret information bits are embedded into the pixels selected by the SIFT algorithm in the blue channel of the color image.

Investigation of Similarity Degree, Between the Container and StegoImages and the Volume of Hidden Secret Information

The degree of similarity between the two compared digital images is determined. Since no detailed explanation is required for this, it is provided briefly. To measure visual quality, the PSNR (Peak Signal-to-Noise Ratio) metric was used.

The comparison of the proposed algorithm with other existing algorithms is given in table 1. The test results for the images, i.e., the PSNR difference values between the container image and the stegoimage, as well as a comparison of the proposed algorithm's PSNR and the volume of secret information bits (HC) embedded in the stegoimage with the newer algorithms developed in recent years, are presented.

Table 1. Comparison of quality indicators of stego images

Input Images	Quality Metrics	(Yong-qing C., et all., 2020)a	(Malik A., et all., 2018)	(Jana B., et all., 2015)	Proposed Algorithms
Lena	PSNR (dB) HC (bits)	34,18 369715	31,93 144887	38,25 223031	41,03 464744
Baboon	PSNR (dB) HC (bits)	24,69 651710	22,85 187141	35,85 273235	40,43 663791
Barbara	PSNR (dB) HC (bits)	32,84 334328	30,26 151269	32,24 241232	43,08 423719
Peppers	PSNR (dB) HC (bits)	32,82 374589	30,42 144177	35,12 232563	39,32 399511
Average	PSNR (dB) HC (bits)	30,62 382087	29,05 189544	32,31 262157	40,96 487941

The average quality metrics for the tested images are HC = 40.96 and PSNR = 44.65. From the table, it is evident that when a larger volume of secret information bits is embedded in the proposed algorithms, higher similarity values (PSNR) are achieved between the container image and the stegoimage compared to the other algorithms. After embedding a large volume of secret information bits, achieving high similarity between the container and stego-images can be considered an advantage of the proposed algorithms.

Moreover, the high PSNR value in the proposed algorithm further demonstrates that when a large number of secret information bits are embedded in the blue channel, visual quality is preserved.

In addition to PSNR values, histogram steganalysis is used for a more precise evaluation of the comparison between the input image and the stegoimage, as well as to assess the robustness of the algorithms.

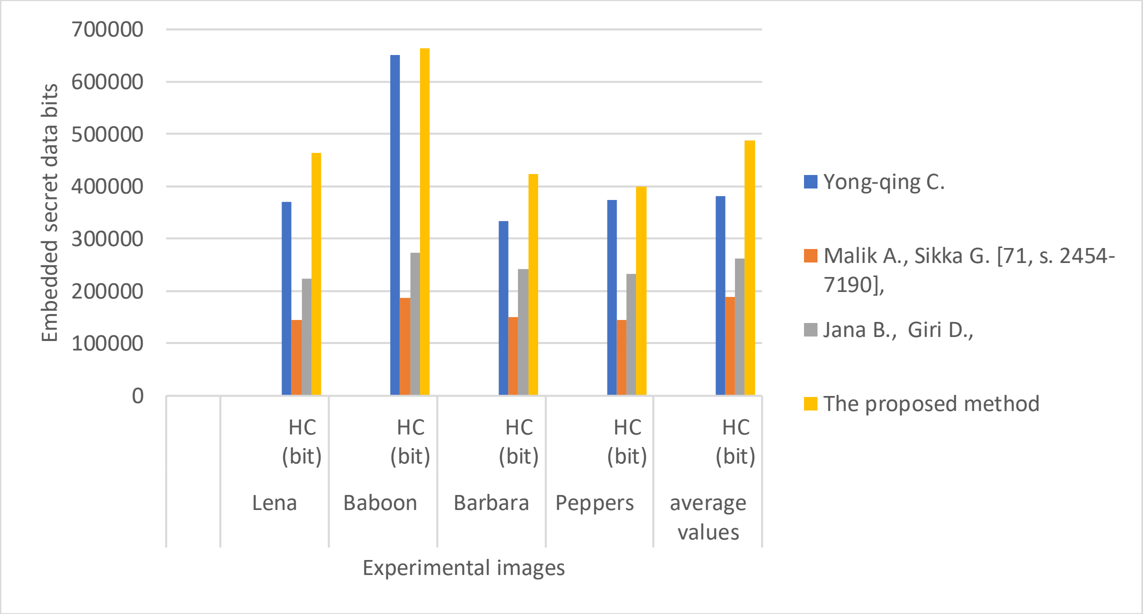


Fig 3. The dependency of embedded secret data bits on the characteristics of various images

Histogram Analysis of the Proposed Method

Histogram is a measure of the frequency of each element in the data space. This widely used statistic is frequently employed in fields such as digital image security, computer vision, and image processing. To generate a histogram, an array of 256 elements, initially set to zero, is defined (this number may vary depending on the bit depth of the image). Each pixel of the digital image is scanned, and the value of the corresponding element in the array is incremented by one. Below is an example of an image and the histogram plot of its gray scale levels.

Histogram steganalysis has been performed on the reference image and stegoimages. Below, the histograms of the container image (Figure 3) and the stegoimage (Figure 4) for the blue color channel are shown. The histograms of other compared images are provided in the appendices.

All the compared images exhibit almost identical histograms. This further proves that the detection of the presence of secret information is nearly impossible. The displayed histograms ensure the effective verification of the stego-images, and no significant changes are observed when compared to the container image histograms.

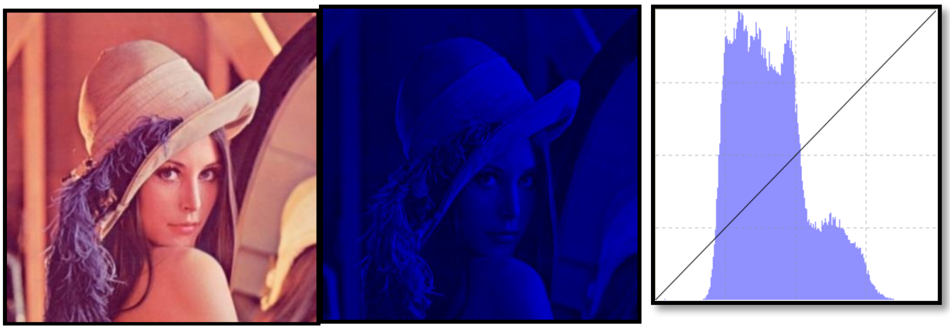


Fig. 4. Container image and the histogram of the blue channel of the container image

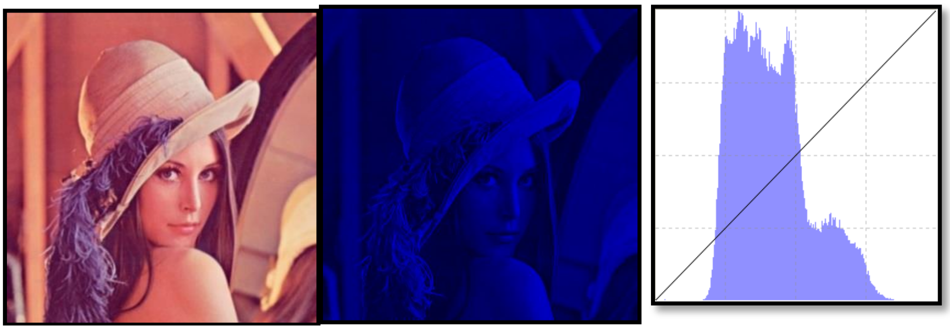


Fig. 5. Stego-image and the histogram of the blue channel of the stego-image

In the histogram, the change in pixel values can be easily understood through the histogram difference, based on how many pixels are included with specific color values.

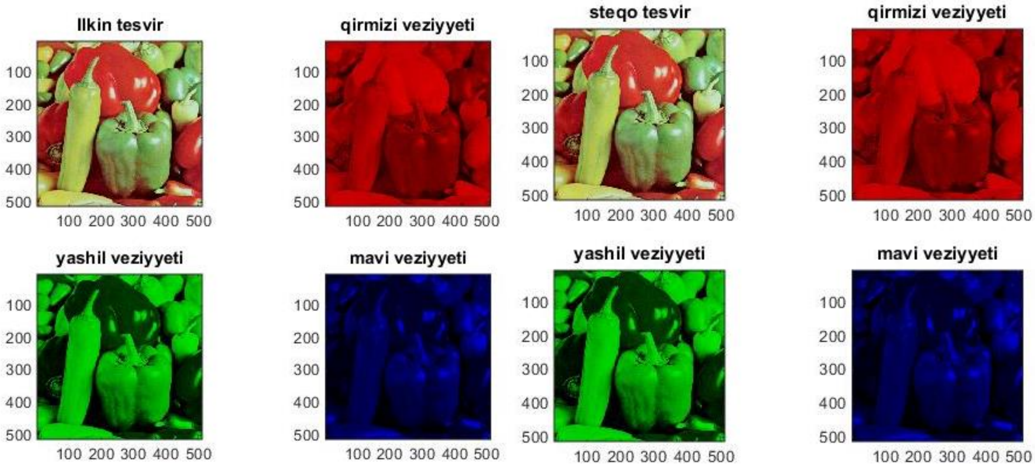
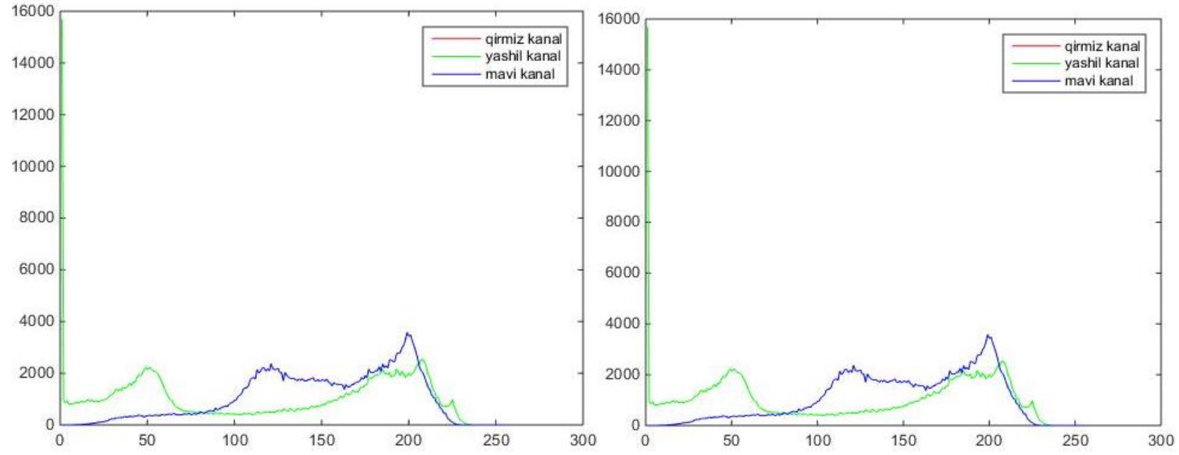


Fig. 6. Container image and stego-image of Peppers



(a) (b)

\

Fig. 7. Histogram of the container image (a), histogram of the stegoimage (b).

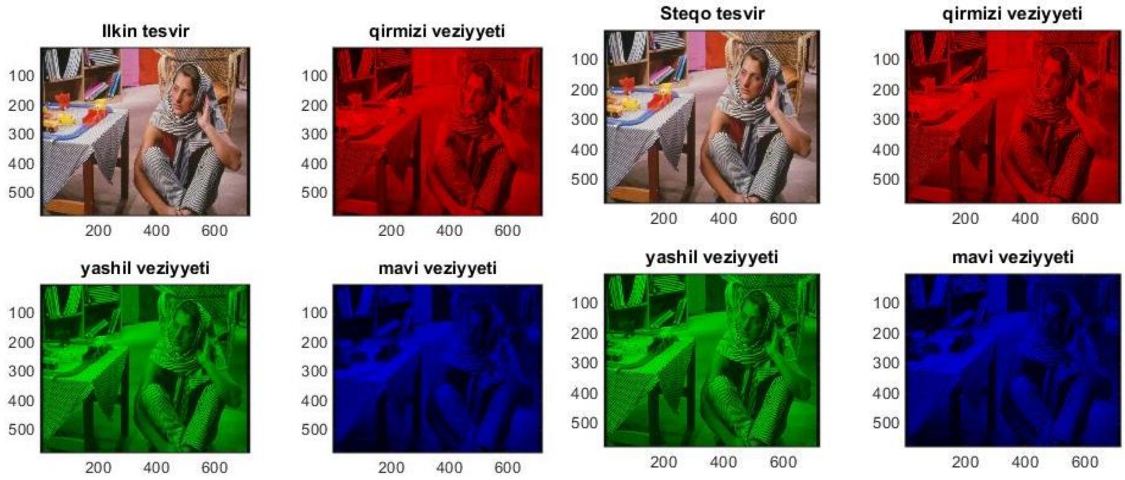
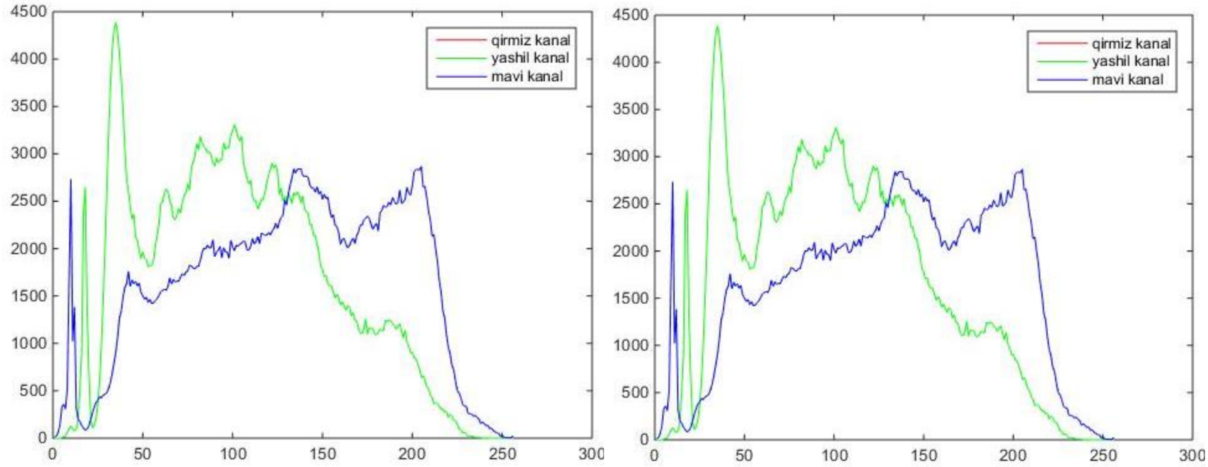


Fig. 8. Container image and stego-image



(a) (b)

Fig. 9. Histogram of the container image (a), histogram of the stegoimage (b).

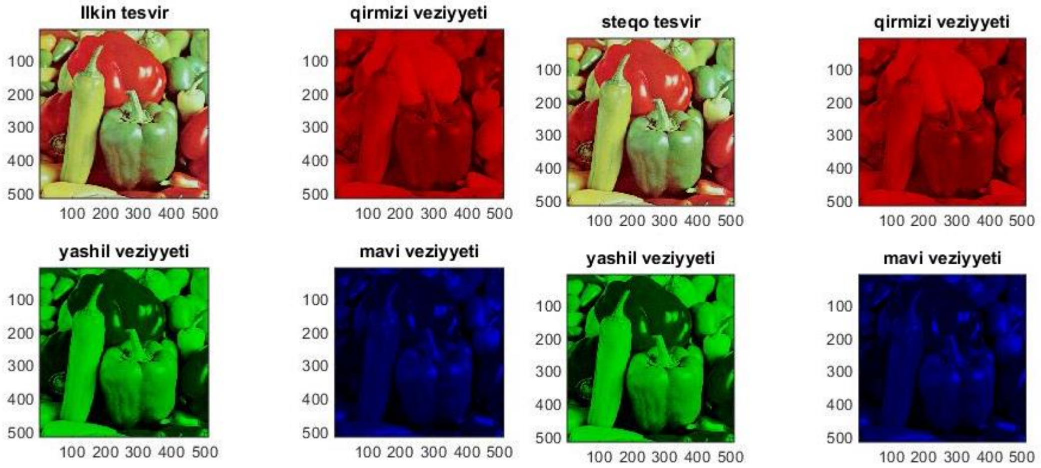
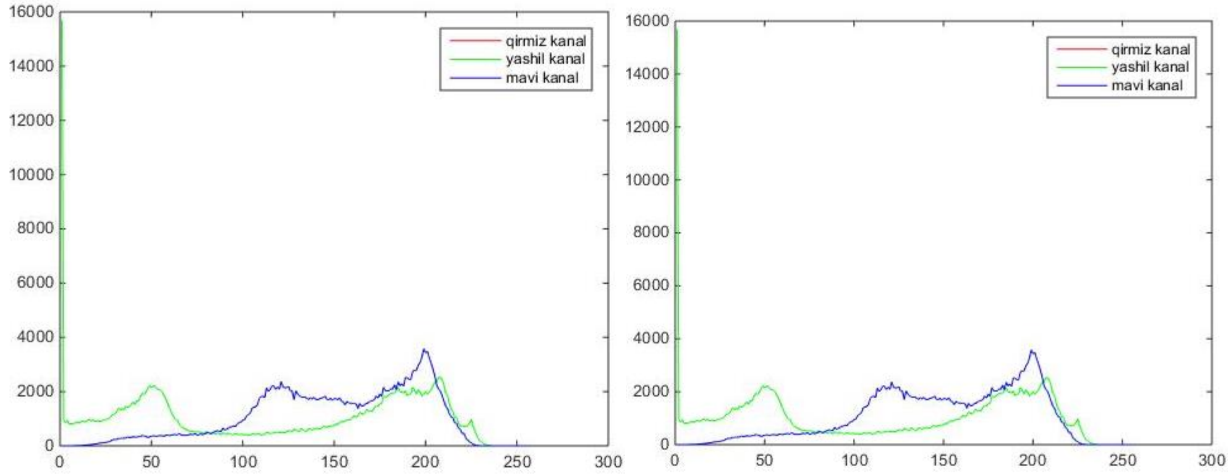


Fig. 10. Container image and stego-image



(b) **(b)**

Fig. 11. Histogram of the container image (a), histogram of the stegoimage (b).

Conclusion and future work

In this algorithm, key point pixels are first identified in the blue channel of the color image using the SIFT algorithm. The use of the SIFT algorithm enhances security in the proposed method. The selection of the blue channel for embedding secret information makes it more challenging to visually detect the hidden data in the stegoimage. Next, the secret information bits are embedded into the container image using the new algorithm. Unlike traditional methods, the octal number system is used during the embedding process, and the stegoimage is generated. In this case, the number of selected bits is higher compared to other steganography algorithms. According to experimental analysis, the algorithm has been proven to meet the quality metrics requirements and to be resistant to many stegoattacks.

From the above, it can be concluded that the proposed secret information hiding algorithm for color images provides a stegoimage with better visual quality and robustness compared to other algorithms in the literature, as well as the ability to hide a larger volume of secret information bits.

In a future works are planned to develop methods that will provide more higher PSNR.

References

1. Abbas, C, Joan, C. Kevi, C. Paul K. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing 90, 727-752.

https://doi:10.1016/j.sigpro.2009.08.010

2. Aziz, F. Ahmad, T Malik, A. Uddin, M. Ahmad, S. Sharaf M., (2020). Reversible data hiding techniques with high message embedding capacity in images. PLoS One, 15(5), 1-24. https://doi.org/10.1371/journal.pone.0231602
3. Bai, J. Chang, C. Nguyen, T. Zhu, C. Liu, Y. (2017). A high payload steganographic algorithm based on edge detection. Displays, 46, 42–51. https://doi.org/10.1016/j.displa.2016.12.004
4. Chen, Y. Sun, W. Li, L. Chang X. Wang, C. (2020). An efficient general data hiding scheme based on image interpolation. Journal of Information Security and Applications, 54, 271–350. https://doi.org/10.1016/j.jisa.2020.102584
5. Guo, F. Yang, J. Chen, Y. Yao, B. (2018). Research on image detection and matching based on SIFT features. 3rd International Conference on Control and Robotics Engineering (ICCRE). Nagoya: IEEE –20-23 April – 2018 (pp. 130-134). https://doi.org /10.1109/ICCRE.2018.8376448
6. Gasimov V., (2019). The Modified Method of the Least Significant Bits for Reliable Information Hiding in Graphic Files. International journal of information security science. 8(1), 1-10.
7. Jana, B. Giri, D. Mondal, S. K. (2015). Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation. Computational Intelligence in Data. Mining 2, 239-248. (Springer). https://doi.org/10.1007/978-81-322-2731-1_22
8. Kim S. Qu X. Sachnev V. Kim H.J. (2019). Skewed histogram shifting for reversible data hiding using a pair of extreme predictions. Trans Circuits Syst Video Technol, IEEE 29 (11), (pp. 3236–3246). https://doi.org/10.1109/TCSVT.2018.2878932
9. Kumar, R, Kim, D. Jung, K. (2019). Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing. Journal Information Security Application 47, 94–103. https://doi.org/10.1016/j.jisa.2019.04.007
10. Lee, D., Kim, S. (2023). Deep learning-based adaptive steganography in RGB images. Multimedia Tools and Applications, 82(6), 7569–7588. https://doi.org/10.1007/s11042-023-14356-9
11. Lu, T.C. Lin, M.C. Huang, C.H. Deng K.M. (2016). Reversible data hiding based on Image interpolation with a Secret message reduction strategy. International Journal of Computer & Software Engineering 1, (pp. 102-112.) https://doi.org/10.15344/2456-4451/2016/102
12. Lien, B. Lin, Y. (2011). High-capacity reversible data hiding by inaximum-span pairing. Multimedia Tools and Applications 52, 499-511.
13. Liang, T. Shuhua, M. Xianchun, M. Hairong, Y. (2022). Research on Image Matching of Improved SIFT Algorithm Based on Stability Factor and Feature Descriptor Simplification. Applied science, Shenyang 17, 1-19. https://doi.org/10.3390/app12178448.
14. Malik, A. Sikka, G, Verm, H.K. (2018). Image interpolation based high capacity reversible data hiding scheme. Multimedia Tools Application 76 (22), 2454-7190. https://doi.org/10.1007/s11042-016-4186-4
15. Mustafayeva, E., Huseynova, G., Gasimov, V., (2019). International journal of information security science. International journal of engineering and applied sciences (ijeas) 6, 32-35.
16. Muhammad, K. Ahmad J. Farman, H. Zubair M, (2015). A novel image steganographic approach for hiding text in color images using HSI color model. Journal of Scientific Research 19, 647-654. https://doi.org/10.48550/arXiv.1502.07808
17. Nağıyeva, A.F. (2023). İnformasiya təhlükəsizliyində steqanoqrafik metodlar. Elmi xəbərlər məcmuəsi, Azərbaycan Texnologiya Universiteti 4, 98 – 104. https://doi.org/10.30546/ATU.4/45.2023.98.
18. Seyyedi, A, Ivanov, N. (2014). A novel Secure Steganography Alqoritm Based on Zero Tree Method. International Journal of Advanced Studies in Computer Science and Engineering 3(3), 1-9.

19. Swain, G. (2018). Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arabian Journal for Scienceand Engineering, 44 (12), 2995–3004.
https://doi.org/10.1007/s13369-018-3372-2
20. Wang, T., Zhang, L., Chen, X. (2021). A perceptual analysis of color channels in image steganography. IEEE Access, 9, 56–70.
https://doi.org/10.1109/ACCESS.2021.1234567
21. Zhang, Z. (2012), Separable reversible data hiding in encrypted image, IEEE Transactions on Information Forensics and Security 7(8), (pp. 553-562).

RƏNGLİ ŞƏKİLLƏRDƏ MƏXFİ MƏLUMATLARI GİZLƏTMƏNİN YENİ ÜSULU

Əbabil Nağıyeva
Azərbaycan Texnologiya Universiteti

Xülasə

Bu məqalədə gizli məlumatların rəngli şəkillərə daxil edilməsi üçün yeni üsul təklif edilir və üsul inkişaf etdirilir. Bu metodun əsas məqsədləri onun etibarlılığını təmin etmək, təsvirin vizual keyfiyyətini və keyfiyyətdə nəzərəçarpacaq dərəcədə pisləşmədən daha böyük həcmdə gizli məlumatı daxil etmək qabiliyyətini qorumaqdır. Bu məqsədlərə nail olmaq üçün metod etibarlılıq problemini həll edən miqyasda dəyişməyən xüsusiyyət transformasiyasından (SIFT) istifadə edir. SIFT metodun miqyaslaşdırma, fırlanma və dəyişən işıqlandırma şəraiti kimi müxtəlif görüntü çevrilmələrinə effektiv şəkildə müqavimət göstərməsini təmin edir.

SIFT həndəsi və fotometrik çevrilmələrə yüksək möhkəmlik təmin etsə də, onun ümumi mövcudluğu da potensial zəifliklər yaradır. Alqoritm və onun nəticələri hamıya məlum olduğundan, təcavüzkarlar steqanaliz üçün axtarış yerini azaldaraq, yerləşdirmə bölgələrini müəyyən etmək üçün eyni üsuldan istifadə edə bilərlər. Bu məhdudiyyəti aradan qaldırmaq üçün gələcək yanaşmalar əsas nöqtələrin təsadüfi pozulmasını, gizli açara əsaslanan seçim metodlarını daxil etməklə və ya SIFT-ni digər transformasiyaya davamlı yerləşdirmə strategiyaları ilə birləşdirməklə təhlükəsizliyi artıra bilər.

Bu yanaşmadan istifadə etməklə, metod təkcə əsas təsvirin xüsusiyyətlərinin qorunub saxlanmasını təmin etmir, həm də gizli məlumatların təhlükəsiz daxil edilməsini asanlaşdırır və bununla da rəngli təsvirlərdə steqaqrafik proseslərin ümumi səmərəliliyini artırır.

Açar sözlər: rəqəmsal steqanoqrafiya, SIFT, təsvir steqanoqrafiyası, məlumatların gizlədilməsi, məxfi məlumat

НОВЫЙ МЕТОД СКРЫТИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЦВЕТНЫХ ИЗОБРАЖЕНИЯХ

Абабиль Нагиева
Азербайджанский технологический университет

Аннотация

В данной статье предложен и разработан новый метод встраивания секретной информации в цветные изображения. Основными целями данного метода являются обеспечение его надежности, сохранение визуального качества изображения и возможность встраивания большего объема секретной информации без заметного ухудшения качества. Для достижения этих целей в методе используется метод масштабноинвариантного преобразования признаков (SIFT), который решает проблему надежности. SIFT гарантирует, что метод эффективно противостоит различным преобразованиям изображений, таким как масштабирование, поворот и изменение условий освещения.

Хотя SIFT обеспечивает высокую устойчивость к геометрическим и фотометрическим преобразованиям, его общедоступность также создает потенциальную уязвимость. Поскольку алгоритм и его результаты широко известны, злоумышленники могут использовать тот же метод для определения областей встраивания, сокращая область поиска для стегоанализа. Для устранения этого ограничения будущие подходы могут повысить безопасность за счет включения рандомизированного возмущения ключевых точек, методов выбора на основе секретного ключа или сочетания SIFT с другими стратегиями встраивания, устойчивыми к преобразованиям.

Используя этот подход, метод не только гарантирует сохранение ключевых характеристик изображения, но и способствует безопасному встраиванию секретных данных, тем самым повышая общую эффективность стеганографических процессов в цветных изображениях.

Ключевые слова: цифровая стеганография, SIFT, стеганография изображений, сокрытие данных, секретная информация

Məqalə daxil olub:	Təkrar işlənməyə göndərilib:	Çapa qəbul olunub
10 aprel 2025-ci il	05 iyun 2025-ci il	30 iyun 2025-ci il