This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2022.Doi Number

Reversible Logic-Based Hexel Value Differencing – A Spatial Domain Steganography Method for Hexagonal Image Processing

Taner Cevik[1], Nazife Cevik[1], Jawad Rasheed[2,3,4], Member, IEEE, Tunc Asuroglu[5], Shtwai Alsubai[6], and Mehmet Turan[7]

[1]Department of Computer Engineering, Istanbul Arel University, Istanbul 34537, Turkey
[2]Deep Learning and Medical Image Analysis Laboratory, Bogazici University, Istanbul 34342, Turkey
[3]Department of Software Engineering, Istanbul Nisantasi University, Istanbul 34398, Turkey
[4]Department of Computer Engineering, Istanbul Sabahattin Zaim University, Istanbul 34303, Turkey
[5]Faculty of Medicine and Health Technology, Tampere University, 33720 Tampere, Finland
[6]Department of Computer Science, College of Computer Engineering and Sciences in Al-Kharj, Prince Sattam Bin Abdulaziz University, P.O. Box 151, Al-Kharj, 11942, Saudi Arabia
[7]Department of Computer Engineering, Bogazici University, Istanbul 34342, Turkey

Corresponding authors: Jawad Rasheed (e-mail: jawad.rasheed@boun.edu.tr), and Tunc Asuroglu (tunc.asuroglu@tuni.fi).

ABSTRACT The field of steganography has witnessed considerable advancements in square-pixel-based image processing (SIP). However, the application of steganography in Hexel (Hexagonal pixel)-based Image Processing (HIP) is still underexplored. This study introduces a pioneering spatial steganography method in the HIP domain called Reversible Logic-Based Hexel Value Differencing (RLBHVD). Our approach draws inspiration from Pixel-Value-Differencing (PVD), a fundamental spatial-domain (S-D) steganography method in SIP. Initially, the image is transformed into the HIP domain using the custom software infrastructure developed for this project. Due to the absence of commercial equipment capable of producing HIP-domain images, traditional digital imaging systems, with their sensor components, analog-to-digital conversion units, and square-pixel-based displays, are employed. Once the image is converted, it is partitioned into standardized heptads, each comprising seven hexels. Simultaneously, the secret message is segmented for embedding into the hexels within each heptad. Unlike SIP-domain PVD, which embeds segments into independent pixel pairs, our method performs iterative embedding within each heptad. Additionally, we leverage Feynman gates, a core element of reversible logic, to achieve retrieval of both the cover image and the secret message. Unlike PVD in SIP, our approach enables reversibility in the recovery process. Experimental results demonstrate that our proposed method, RLBHVD, outperforms its SIP counterpart, PVD, by achieving a low Mean Squared Error (MSE), high Peak Signal-to-Noise Ratio (PSNR), and significant similarity between the stego-image and cover image histograms. These findings highlight the efficacy and superiority of our HIP-based steganography approach in comparison to existing SIP methods.

INDEX TERMS Heptad, hexel, hexagonal image processing, pixel-value-differencing, reversible logic-based hexel value differencing, steganography.

I. INTRODUCTION

Communication security has become more critical than ever because of the widespread use of growing multimedia transmission through the internet. Two methods are used to accomplish communication security: encryption and data hiding (DH). Although both methodologies primarily serve to protect data, the way to hide the data and the appearance of the hidden data is different. By its very nature, Cryptology does not hide from the environment in which the data is encrypted. The goal is not to hide that the data is encrypted but to hide the data. However, this is not the case for DH. The main goal of DH is not to encrypt data but to conceal that the data is stored by embedding data into other data in a way that is not visible from the outside [1]. DH is the generic name given to techniques applied to hide data in another digital medium in a way not to be noticed by outsiders. DH has found broad application areas such as copyright protection, content authentication, and secret communication to be utilized in military, commercial, anti-criminal, etc. [2][3].

Steganography is a branch of DH that embeds secret data, such as text, images, etc., into a cover media to conceal its

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

existence [4]–[8]. Steganography, a term derived from the Greek words "Stegos" and "grafia" which means “secret”, and “writing”, respectively, involves concealing confidential data within digital images [9]. This technique relies on the use of a cover image, which carries the hidden data, thus constructs the stego-image that contains the embedded information. A high-quality steganography method aims to minimize falsification in the cover image derived by the embedding course and ensure that the confidential data remains undetectable in the resulting stego-image [10]–[12].

Image processing involves emulating human vision and applying it to computer vision. In the real world, light data is continuous and collected through distinct sensors that are sensitive to different parts of the light spectrum. Such sensors are arranged in rectangular or square arrays. However, since smart processor-based computing machines can only operate digital data, the continuous light data needs to be sampled and converted into digital form. The type of sensor array used impacts the downstream processing performed by the computer. For rectangular or square sensor arrays, the digital data unit created is called a pixel, which is square in shape.

Alternatively, sampling light data on a hexagonal lattice and dealing with it within a hexagon domain can yield promising results and lead to various improvements. The use of hexagonal geometry in image processing has been under study for many years. Initially, hexagons were not considered the most efficient approach to segment a plane into equal-sized regions until Hales [13][14] demonstrated otherwise. Natural occurrences of hexagonal arrangements, such as photoreceptors in the fovea and honeycombs [15], also showcase the significance of hexagonal geometry. Compared to the square lattice architecture, the hexagonal lattice offers several advantages. Its superior radial symmetry allows circular symmetric kernels, enhancing the accuracy of detecting both curved and straight edges. Additionally, its lattice format ensures local equality and uniqueness, further benefiting the image processing tasks [16][17].

The HIP field has received limited attention primarily due to the absence of a mathematical framework, crucial hardware, and software infrastructure dedicated to handling hexels. Despite this, exploring HIP can potentially address data capacity limitations thus speeding up processing. Moreover, HIP shows promise in enhancing the output quality of standard SIP procedures such as edge detection, segmentation, and object recognition, making it an appealing area for further investigation. Despite steganography having a long history in the SIP domain, no prior attempts have been made to exercise and evolve it specifically in the HIP domain, highlighting a potential area for future research and innovation.

- To our knowledge, no steganography approach for the HIP domain has yet been suggested. This study is the first of its kind in this area. This study presents an S-D-data hiding approach, Reversible Logic Based Hexel Value Differencing (RLBHVD), in the HIP domain.

The data that can be concealed in the material and the degree of change between the original version and the new material resulting from this data hiding are the two most critical factors that influence the performance of a data-hiding method. The simulation results demonstrated that steganography performed in the HIP outperforms steganography conducted in the SIP, as it allows for higher data hiding capacity and less perceptible changes to the material after data embedding. The findings suggest that utilizing the Hexagonal Image Processing domain offers advantages in terms of data concealment efficiency and visual quality preservation.

In order to allow readers to comprehend the research methodology and findings effectively, the article's structure is as follows: Section II summarizes the basics and related research done in steganography. Section III provides an overview of the principles of conventional SIP-domain PVD. In Section IV, the proposed RLBHVD method is outlined. Section V details the dataset utilized for testing, the experimental setup, and the discussions of the achieved results. Lastly, Section VI outlines the conclusions drawn from the study and potential future research directions.

II. RELATED WORKS

Steganography is a multifaceted discipline that enables covert communication by concealing data within seemingly unrelated carriers. This intricate practice combines artistic ingenuity with scientific methodologies to safeguard sensitive information during transmission and storage. In contrast to encryption, steganographic messages are not noticed because the data is hidden from the human eye [17]. The proliferation of the World Wide Web has led to a substantial surge in the utilization of digital images across various online platforms. This widespread adoption of digital imagery signifies its pivotal role in modern communication, information sharing, and visual content dissemination. Images are preferred for embedding steganographic data due to the several redundant bits in the digital depiction of the image. There are many different image file formats within the digital image domain. Different steganography techniques exist for each image format [18].

Recent advancements in steganography focus on strategically placing hidden data within the edges or texture regions of cover images, aiming to maintain the cover image's integrity. Nevertheless, despite these efforts, traces of alterations often remain, making it challenging to escape detection through statistical analysis. Even when concealed within the carrier image's redundant texture regions, preventing the detection of the hidden message proves to be a daunting task. As a result, standard steganography techniques provide a concealed security risk. To significantly thwart steganalysis identification, researchers [19][20] developed the concept of implicit information masking. This concept is based on the principle that the cover image is generated by exploiting the secret message.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

Developing an innovative data hiding system that balances optimal robustness, high hiding capacity, visual quality, and steganographic security presents a complex technical hurdle. Consequently, researchers have dedicated significant efforts to explore steganography comprehensively, leading to a plethora of proposed methods in academic literature.

Image-based steganography techniques can be largely categorized into model-based steganography, spread spectrum, transform domain, and S-D, each offering distinct approaches to concealing information within digital images. This ongoing research and classification aim to enhance data security and privacy in various applications [21].

In the realm of data hiding, concealing a covert message within the S-D of pixel values is a common practice. Among various embedding techniques, the least significant bit replacement method (LSB) stands out for its popularity, thanks to its simplicity and low CPU overhead. Nonetheless, LSB embedding exhibits inherent flaws, as it causes imbalanced distortion in pixels depending on their parity. This makes it vulnerable to detection through steganalysis [21][22].

The LSB replacement method is asymmetric. For steganalysis, this asymmetry is exploited. Some detectors are known to detect LSB [23]. To address these issues of distortion produced by LSB substitution, Chan et al. [24] proposed an elegant solution in 2004: the Optimum Pixel Adjustment Procedure (OPAP). This approach involves encoding message bits in the rightmost LSBs of a ---bit pixel while assessing and modifying the other bits accordingly. By carefully adjusting the remaining bits, the method aims to minimize distortions, thereby reducing the detectability of the hidden data. In essence, OPAP offers an efficient means to counteract the shortcomings of LSB substitution and achieve more secure and inconspicuous data hiding.

Sharp devised a data-concealing approach dubbed the LSB matching scheme to circumvent the LSB substitution scheme's asymmetry [25]. Unlike the latter, the LSB Matching method (LSBM) doesn't directly oust the LSB of an overlay pixel with a secret bit. Rather, it cleverly modifies the coverage pixel by either incrementing or decrementing it by one at random if the secret bit doesn't match its LBS. By doing so, the distinction between odd and even pixels becomes less evident, making it considerably more challenging for statistical detectors to identify LSBM compared to LSB detection [26]. This technique has gained widespread recognition for its ability to enhance the security and complexity of steganographic applications.

Mielikainen introduced the LSB matching revisited (LSBMR) [27] that successfully eliminates the asymmetry present in the LSBR, ensuring comparable visual quality and concealing capabilities. In LSBMR, two secret bits are concurrently embedded into a pair of cover pixels using binary functions and four embedding criteria. This modification results in an identical payload as the original LSBM method but with fewer alterations made to the cover image. In terms of performance, their scheme boasts an expected number of modifications per pixel of 0.375, outperforming the LSBM method, which has a performance rate of 0.5. Correspondingly, the visual aspect, as evaluated by peak signal-to-noise ratio (PSNR), is notably superior in the LSBMR approach. On the other hand, LSBMR is detected by Ker's [26] suggested detector.

Zhang and Wang [28] proposed an innovative enhancement to Mielikainen's exploiting modification direction (EMD) technique. This improvement enables encoding a message digit within a 5-ary notational system to be achieved using just one pixel in a pixel pair. By leveraging this modification direction approach, the efficiency of data concealment is significantly increased, making it a promising advancement in steganography methods.

By incorporating LSB-M and EMD algorithms into the classic LSB approach, significant enhancements can be achieved, leading to higher stego picture quality while maintaining the same payload. However, it is important to note that LSB matching and EMD have inherent limitations, with maximum payloads of only 1 and 1.161 bits per pixel (bpp), respectively. Consequently, such techniques are not appropriate for applications that demand a large payload capacity. Regrettably, there are no means to further increase the payload using the embedding techniques of LSB matching and EMD, making them less effective for scenarios requiring extensive data concealment capabilities [29].

The Pixel-Value-Differencing (PVD) [30] scheme is a steganographic technique that calculates the charge by analyzing the disparity between consecutive pixels. By selecting two pixels and utilizing a quantization range table, PVD ensures high imperceptibility in steganographic images, making the embedded data difficult to detect visually. One of the key advantages of PVD is its ability to accommodate various payloads, allowing for the concealment of substantial amounts of data within the image. Furthermore, PVD excels in preserving the original image's characteristics even after data embedding, ensuring that the visual quality remains intact. As a result, researchers have shown great interest in recent times, exploring different avenues to enhance and optimize the PVD scheme, leading to further advancements and innovations in the field of steganography [31]–[34].

III. REVIEW OF PVD

In LSB-based steganography, a widely recognized S-D technique, the LSBs of a cover image are altered in a pseudo-random manner, following the secret bitstream to be incorporated. Such approaches assume that each pixel in an image can bear the same amount of change without creating visual artifacts. This is not the case, particularly in images comprising smoother and regular areas [35]. In general, pixels on the edges of an image can accept more changes than those on the smooth side. In smooth parts, the range of changing pixel values is limited. However, it is broad in edge areas, ensuring that the stego-image retains acceptable perceptual quality [36].

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

Based on the idea that edge parts in an image may hide a higher quantity of data than smooth regions, Wu and Tsai [30] introduced the PVD. The image is partitioned into non-overlapping and successive groups of two nearby pixels in PVD. Secret information is concealed in these different values.

The first stage in PVD is to create a range table (Table I) with n contiguous ranges (R_k, where $k = 1, 2, \ldots, n$), having a table range of 0 to 255. R_k's lower and upper boundaries are represented by l_{R_k} and u_{R_k}, respectively, which yields $R_k \in [l_{R_k}, u_{R_k}]$. The width of R_k, that is, $w_k = u_{R_k} - l_{R_k} + 1$, determines how many bits ($\lfloor \log_2 w_k \rfloor$) may be concealed in two successive pixels. The original range table is necessary to extract the encoded secret data since R_k is intended as a variable [3], [32], [37]–[39].

The cover image pixel-pair undergoes an update process to transform into the stego-image pixel-pair, following the (1) [34]:

$$(p_i', p_{i-1}') = \begin{cases} \left(p_i + \left\lceil \frac{d_i' - d_i}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor\right), if\ (p_i \geq p_{i+1}, d_i' > d_i) \\ \left(p_i - \left\lceil \frac{d_i' - d_i}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor\right), if\ (p_i < p_{i+1}, d_i' > d_i) \\ \left(p_i - \left\lceil \frac{d_i' - d_i}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor\right), if\ (p_i \geq p_{i+1}, d_i' \leq d_i) \\ \left(p_i + \left\lceil \frac{d_i' - d_i}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor\right), if\ (p_i < p_{i+1}, d_i' \leq d_i) \end{cases} \quad (1)$$

Algorithm I expresses the pseudocode of the PVD data embedding process.

Figure 1 highlights the data-embedding process of PVD, offering insight into how it operates on a sample pixel pair. However, on the receiver side, the extraction of the hidden message is relatively straightforward compared to the embedding stage.

The extraction process involves utilizing the range table to retrieve the embedded message from the stego-image, as depicted in Figure 2. This clear flow of the extraction process on a sample stego-pixel pair simplifies the task of recovering the secret information concealed using the PVD method.

IV. THE PROPOSED RLBHVD

HIP poses significant complexity and challenges due to the absence of adequate hardware, algebraic techniques, and software infrastructure tailored to this domain. To work effectively in HIP, all concepts applicable in traditional SIP must be adapted and extended to have equivalent counterparts. As mentioned above, image steganography started to be applied in the S-D, and the most basic of the steganographic methods are again the methods in this S-D. PVD is also one of the most fundamental, widely used, and variant-derived approaches in S-D steganography, having paved the way for many following investigations [40]–[42].

This research addresses a significant gap in the field of steganography by introducing a pioneering method specifically designed for the HIP domain. As per our knowledge, prior to this study, no other steganography techniques have been put forth for HIP, making this investigation a pioneering contribution to the area.

A. EMBEDDING PROCEDURE

In the ordinary PVD, the cover image is segmented into pairs of pixels. In RLBHVD, Nonetheless, the cover image is partitioned into heptad of hexels, each as illustrated in Figure 3.

Once the cover image is partitioned into heptads, the hexel in the center of each heptad is called the reference hexel, and all stenographic operations are built on this reference hexel. Steganography is done on the pixels that comprise each pair in ordinary PVD.

TABLE I
THE QUANTIZATION RANGE TABLE

R_k	R_1	R_2	R_3	R_4	R_5	R_6
Range (R)	[0 – 7]	[8–15]	[16 – 31]	[32 – 63]	[64 – 127]	[128 – 255]
Width (m)	8	8	16	32	64	128
Capacity (t)	3	3	4	5	6	7

ALGORITHM I

PVD data embedding

function: PVD_Data_Embed(*img*, *msg*, *R*):*stgImg*

Input: *img* – Cover Image
msg – Binary Secret Message
R – Range Table

Output: *stgImg* – Stego Image

r = size(*img*,1)
c = size(*img*,2)
ml = length(*msg*)
for *i* =1 to *r*-1 **do**
  for *j* =1 to *c*-1 **do**
  if (*ml* > **0**) **then**
    $d = |img_{i,j+1} - img_{i,j}|$
    $k \rightarrow \min_k(u_{R_k} - d)$
    $w_k = u_{R_k} - l_{R_k} + 1$
    $t = \lfloor \log_2 w_k \rfloor$
    msg_t = Extract_t_bits(*msg*)
    b = binTodec(msg_t)
    $d' = l_{R_k} + b$
    $m = |d' - d|$
    if $img_{i,j} \geq img_{i,j+1}$ **&&** $d' > d$ **then**
      $stgImg_{i,j} = img_{i,j} + \left\lceil \frac{m}{2} \right\rceil,\ stgImg_{i,j+1} = img_{i,j+1} - \left\lfloor \frac{m}{2} \right\rfloor$
    else if $img_{i,j} < img_{i,j+1}$ **&&** $d' > d$ **then**
      $stgImg_{i,j} = img_{i,j} - \left\lceil \frac{m}{2} \right\rceil,\ stgImg_{i,j+1} = img_{i,j+1} + \left\lfloor \frac{m}{2} \right\rfloor$
    else if $img_{i,j} \geq img_{i,j+1}$ **&&** $d' \leq d$ **then**
      $stgImg_{i,j} = img_{i,j} - \left\lceil \frac{m}{2} \right\rceil,\ stgImg_{i,j+1} = img_{i,j+1} + \left\lfloor \frac{m}{2} \right\rfloor$
    else
      $stgImg_{i,j} = img_{i,j} + \left\lceil \frac{m}{2} \right\rceil,\ stgImg_{i,j+1} = img_{i,j+1} - \left\lfloor \frac{m}{2} \right\rfloor$
    end if
    msg = *msg*(*t*:length(*msg*))
    ml = length(*msg*)
  end if
 end for
end for
return *stgImg*

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

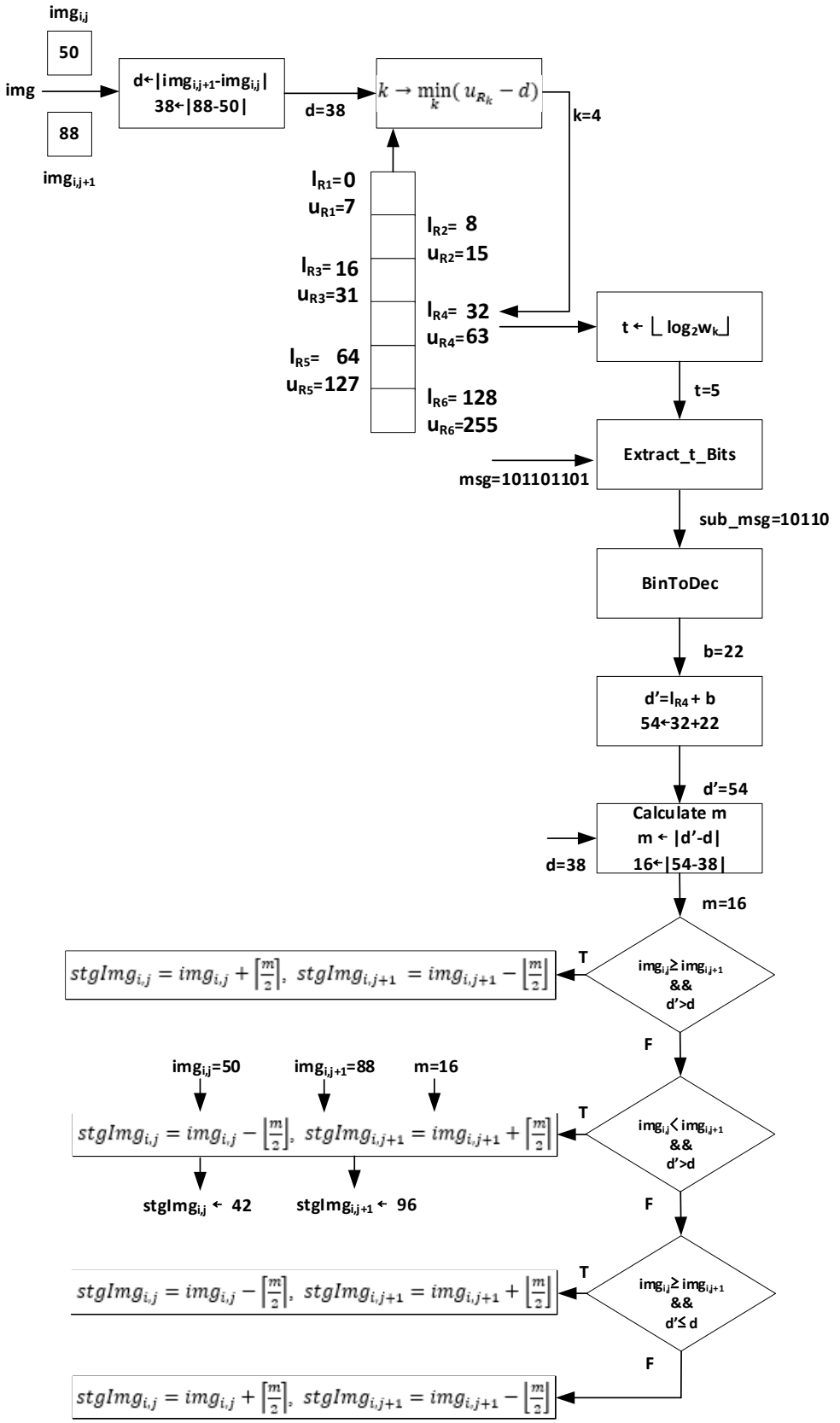


FIGURE 1. **An example implementation of the PVD data-embedding process.**

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

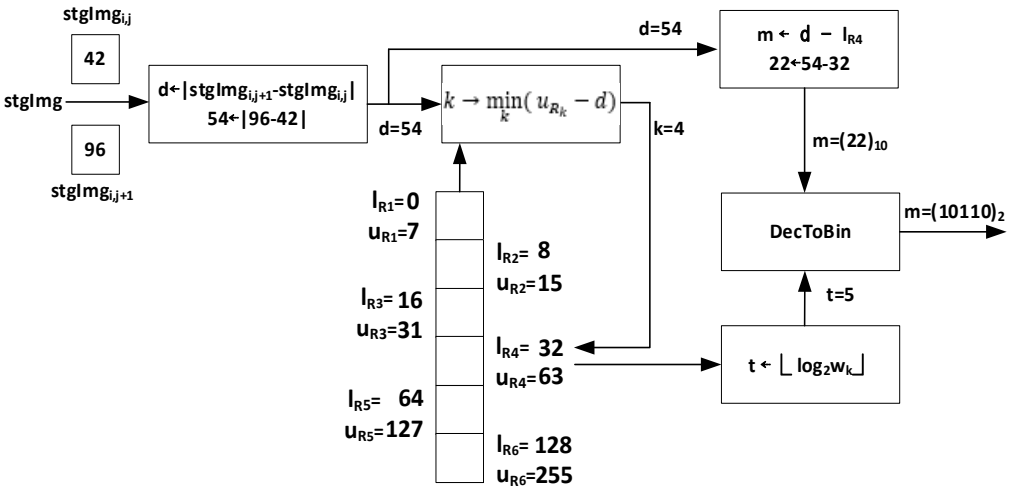


FIGURE 2. **An example implementation of the PVD data-extraction process.**

Thus, each pair has one steganographic operation. In RLBHVD, on the other hand, each heptad has six steganographic processes. Unlike the ordinary PVD, message embedding is done into only one of the hexels, not both. Thus, the center hexels of the heptads never change. The steganographic process in a heptad is formalized in (2) as follows:

$$\begin{Bmatrix} (hr, hr_{ngb1}') = RLBHVD(h_r, hr_{ngb1}) \\ (hr, hr_{ngb2}') = RLBHVD(h_r, hr_{ngb2}) \\ (hr, hr_{ngb3}') = RLBHVD(h_r, hr_{ngb3}) \\ (hr, hr_{ngb4}') = RLBHVD(h_r, hr_{ngb4}) \\ (hr, hr_{ngb5}') = RLBHVD(h_r, hr_{ngb5}) \\ (hr, hr_{ngb6}') = RLBHVD(h_r, hr_{ngb6}) \end{Bmatrix} \quad (2)$$

In PVD, a sub-message is retrieved from the entire message and embedded into both pixels by sharing according to the disparity between pixel intensity values. However, in RLBHVD, the embedding process is reversible after defining the sub-message to be embedded according to the methodology of PVD. Reversibility is provided by exploiting the Feynman gates [43], one of the primary elements of reversible logic. Using the Feynman gate, the stego-hexel and reference hexel of the heptad are fed into the Feynman gate, and the original sub-message is correctly extracted. The implementation of message embedding on a single hexel pair is illustrated in Figure 4.

Figures 5-6, and Algorithm II show the schematic representation of the entire heptad embedding process, the implementation of RLBHVD on the sample heptad given in Figure 3, and the pseudocode of the RLBPVD message embedding process, respectively.

B. EXTRACTION PROCEDURE

The message extraction process is carried out separately for each heptad. At each heptad, the extraction step begins with the (hr, hr_{ngb_6}) hexel-pair. The actions used throughout the embedding process are reversed this time to get the original intensity value of the central hexel at the present process.

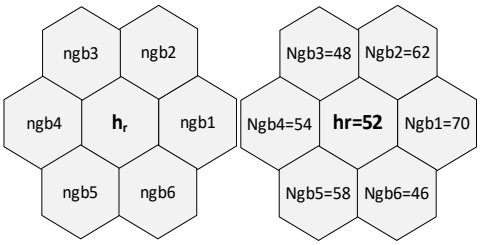


FIGURE 3. **An example heptad of hexels.**

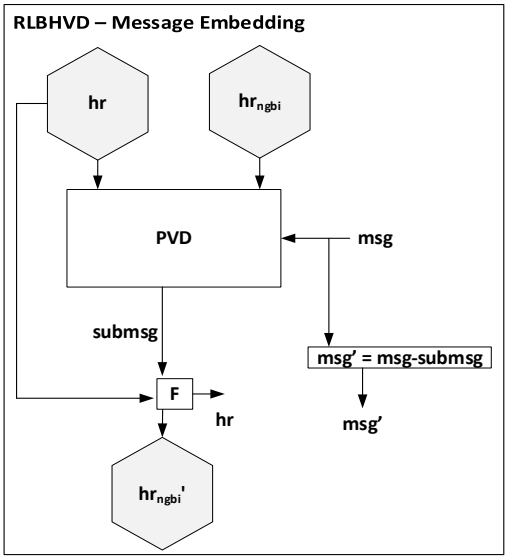


FIGURE 4. **The schematic representation illustrating the sequential process involved in embedding a single RLBHVD message can be observed through the flow diagram.**

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

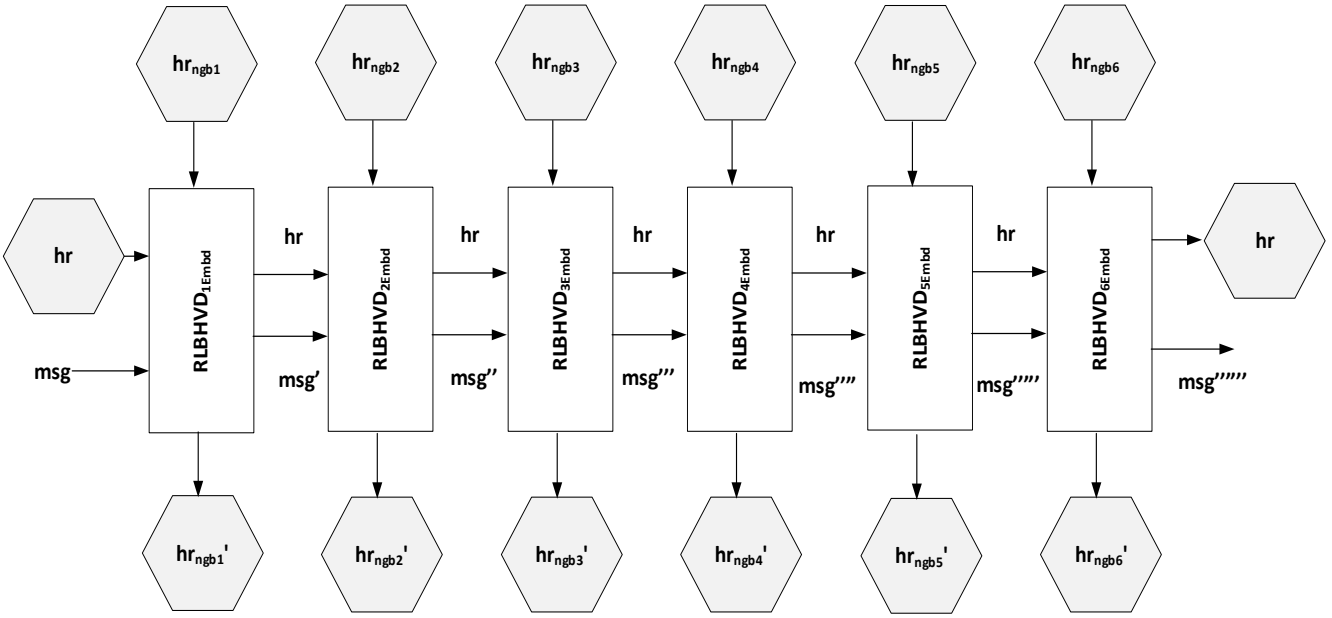


FIGURE 5. **The flow diagram of the entire heptad message embedding process.**

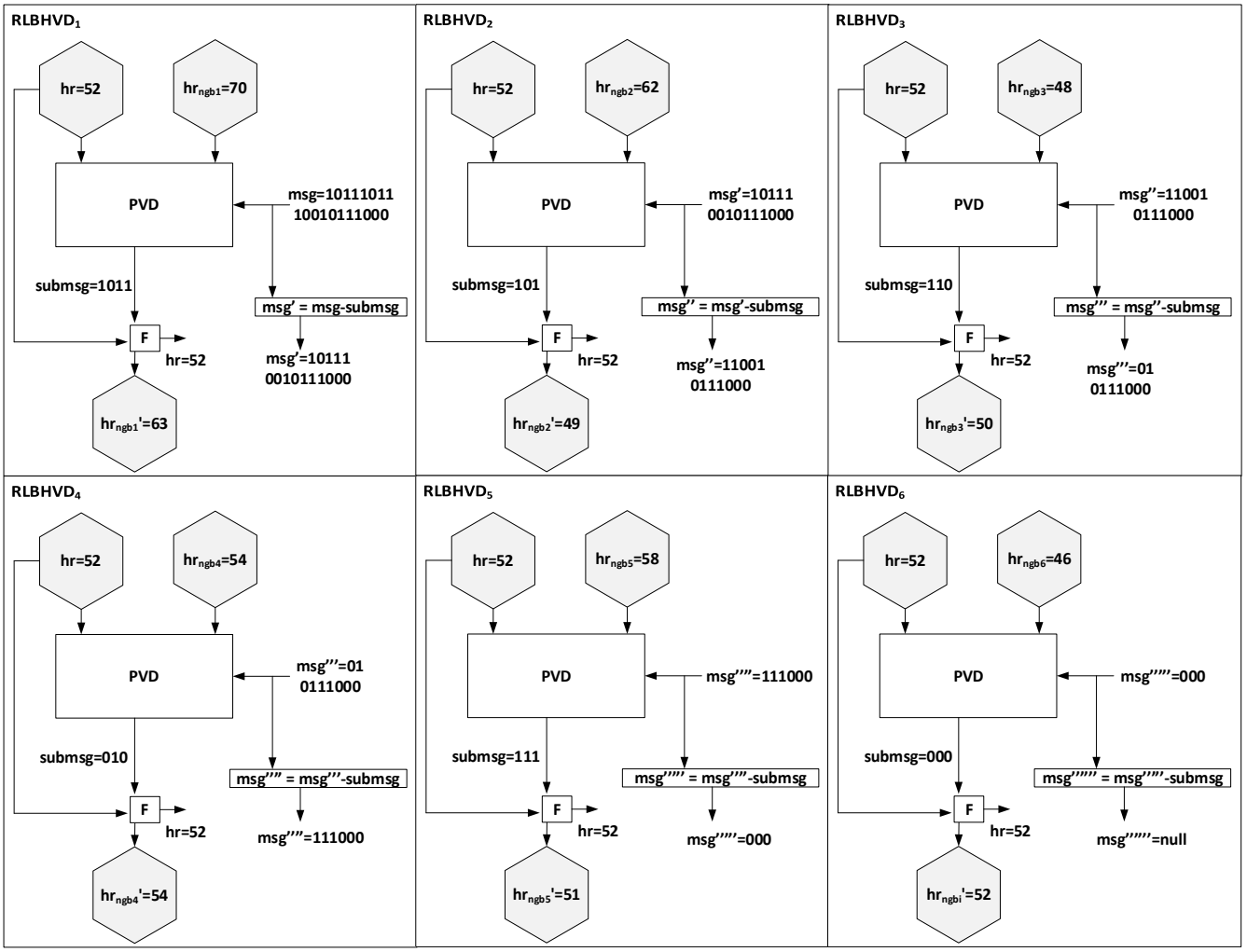


FIGURE 6. **Implementation of RLBHVD message embedding on the sample heptad, given in Figure 3.**

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

ALGORITHM II

Single RLBHVD message embedding on a hexel pair

function: RLBHVD_Data_Embed(*img*, *msg*, *R*): *stgImg*
  Input: *img* – Cover Image
    msg – Binary Secret Message
    R – Range Table
  Output: *stgImg* – Stego Image
  Heptads = GetHeptads(*img*)
  ml = length(*msg*)
  for each heptad *h* in *Heptads* **do**
    hr = hexel_center(*h*)
    for *i* =1 to 6 **do**
      if (*ml* > **0) then**
        $d = |hr - hr_{ngbi}|$
        $k \rightarrow \min_{k}(u_{R_k} - d)$
        $w_k = u_{R_k} - l_{R_k} + 1$
        $t = \lfloor \log_2 w_k \rfloor$
        msg_t = Extract_t_bits(*msg*)
        b = binTodec(msg_t)
        $(hr, hr_{ngbi}) = Feynman(hr, b)$
        msg = *msg*(*t* : length(*msg*))
        ml = length(*msg*)
      end if
    end for
  end for
  stgImg= combineHeptads(*Heptads*)
return *stgImg*

The secret message is extracted by explicitly inverting the implementation order of the embedding operation, this time on the receiver side because the Feynman gate is reversible. Unlike the embedding process in which individual embedding steps are done sequentially, the individual extraction steps on a heptad are done in parallel. That is because the message to be extracted does not depend on the extracted message of the previous-on-operated hexel-pair. Algorithm III, Figures 7-8 show the pseudocode of the RLBPVD data extraction process, implementation of message extraction on a single hexel pair, and entire heptad message extraction process, respectively.

V. EXPERIMENTAL RESULTS AND DISCUSSION

In the system having Intel Core i9-10900KF CPU @3.70 with 64 GB RAM features, the hidden data-carrying capacity of RLBPVD, the steganography method we developed for the HIP domain, and the discrepancies between the produced stego-image and original image are investigated via MATLAB. The simulations use images from the USC–SIPI database [44], Lena, a Baboon, an Airplane, a Sailboat, House, and Peppers as the cover images. The images are first scaled to 256×256 and then converted to grayscale. The simulations use two gray-value-difference range sets $(8, 8, 16, 32, 64, 128)$, and $(2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64)$.

ALGORITHM III

Single RLBHVD message extraction on a hexel pair

function: RLBHVD_Data_Extract(*stgImg*):*msg*
  Input: *stgImg* – Stego Image
  Output: *msg* – Secret Message
  Heptads = GetHeptads(*img*)
  for each heptad *h* in *Heptads* **do**
    hr = hexel_center(*h*)
    for *i* =1 to 6 **do**
      $(hr, b) = Feynman(hr, hr_{ngbi})$
      msg = *msg* + *b*
    end for
  end for
return *msg*

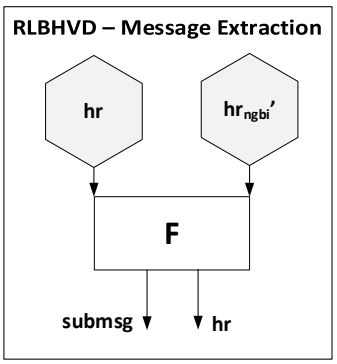


FIGURE 7. The flow diagram of a single RLBHVD message extraction step.

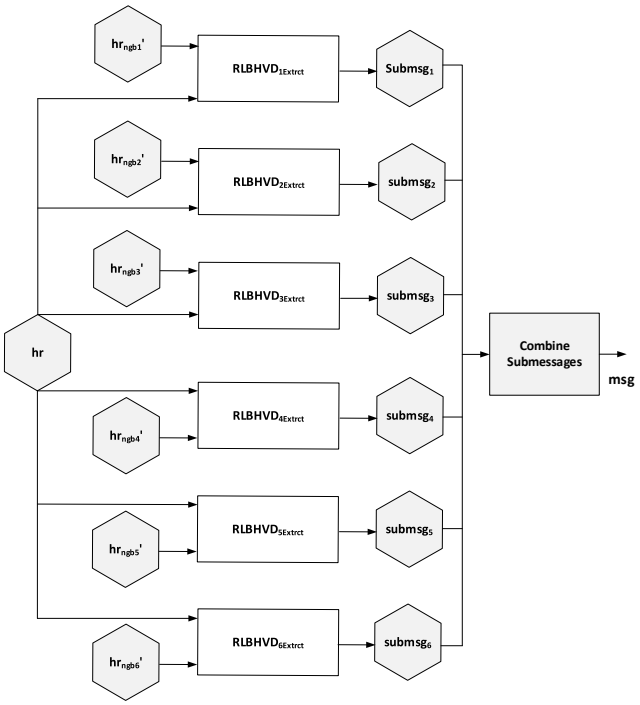


FIGURE 8. The flow diagram of the entire heptad message extraction process.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

A pseudo-random number generator generates the secret message in the bitstream format. The change in visual perception following message embedding is demonstrated in the first stage. A sample cover image, Lena, its message-embedded variants (stego-images), and the visual changes between them regarding the range tables abovementioned are shown in Table II. PVD_Sq, RLBHVD refers to the ordinary PVD steganography for the SIP domain [30] and our proposed steganography method for the HIP domain, respectively. Pixels on the difference image lay in the directions 0°, 60°, and 120° since the HIP domain is established on these angular directions, and RLBHVD embeds secret message bits by considering the hexel relations in these directions. Another essential point to be mentioned is that since the entire range $[0-255]$ is partitioned into a smaller and higher number of intervals in the second range table $(2,2,4,4,4,8,8,16,16,32,32,64,64)$ than the first range table $(8,8,16,32,64,128)$, less secret message bits are embedded to the cover image.

In the next stage of the analysis, the secret message embedding capacity of PVD_Sq and RLBHVD and the similarity between the cover images and their corresponding stego-images created as the result of these steganography methods are measured. The capacity is measured by the average number of bits embedded in each pixel (BPP) in the cover image. Three essential metrics, PSNR, SSIM, and histogram intersection [45][46], are considered for the similarity analysis. As seen in Table III, the message carrying capacity decreases when the range table $(2,2,4,4,4,8,8,16,16,32,32,64,64)$ is utilized, which also consolidates Table II.

Fewer bits are embedded due to narrower intervals in the tables for each pixel pair in PVD_Sq and each hexel pair in RLBHVD. RLBHVD outperforms PVD_Sq regarding message embedding capacity, which naturally comes at a cost. As the number of embedded bits rises, similarity metrics, PSNR, SSIM, and histogram-intersection-ratio decrease. The histogram comparison of the stego-image and cover image is made visually, as illustrated in Figure 9. A range table $(2,2,4,4,4,8,8,16,16,32,32,64,64)$ reduces the number of embedded-secret-message-bits, reducing the proportion of non-overlapping regions in the histograms of the stego-images and their related cover images.

We also conducted a performance analysis of earlier research in the literature that was inspired by PVD to compare the performance of the proposed method. The first study we compared is Digital Image Steganography Using Eight-Directional PVD (8D_PVD) which was proposed by Swain [47]. 8D_PVD uses LSB substitution while also making use of the edges in eight different directions. A modified LSB substitution technique is used to embed 3 or 4 bits of data into the middle pixel of each 3×3-pixel block. Then, eight difference values with eight nearby pixels are computed using the updated value of the center pixel.

TABLE II
DEMONSTRATION OF THE VISUAL CHANGES BETWEEN THE COVER IMAGE LENA AND ITS MESSAGE-EMBEDDED VARIANTS (STEGO-IMAGES) FOR THE TWO RANGE TABLES, (8,8,16,32,64,128) AND (2,2,4,4,4,8,8,16,16,32,32,64,64)

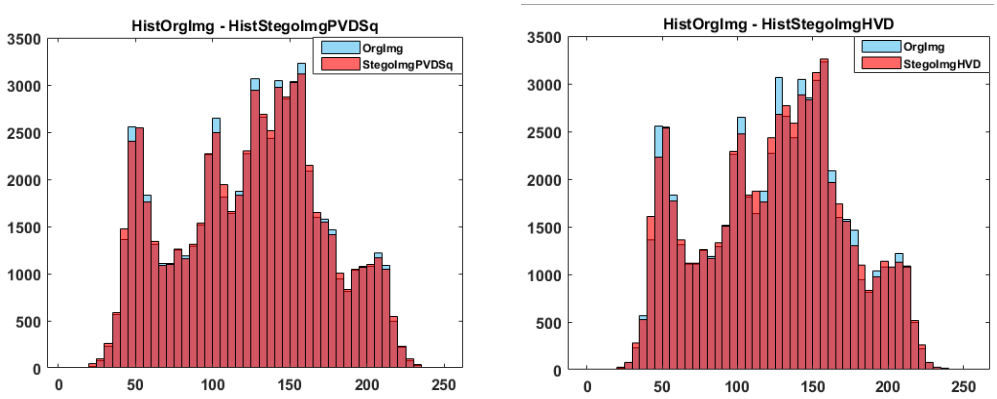
Image	Cover Image	StegoImage	Cover Image – Stego Image
Lena $(PVD_Sq)_{RT1}$			
Lena $(RLBHVD)_{RT1}$			
Lena $(PVD_Sq)_{RT2}$			
Lena $(RLBHVD)_{RT2}$			

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

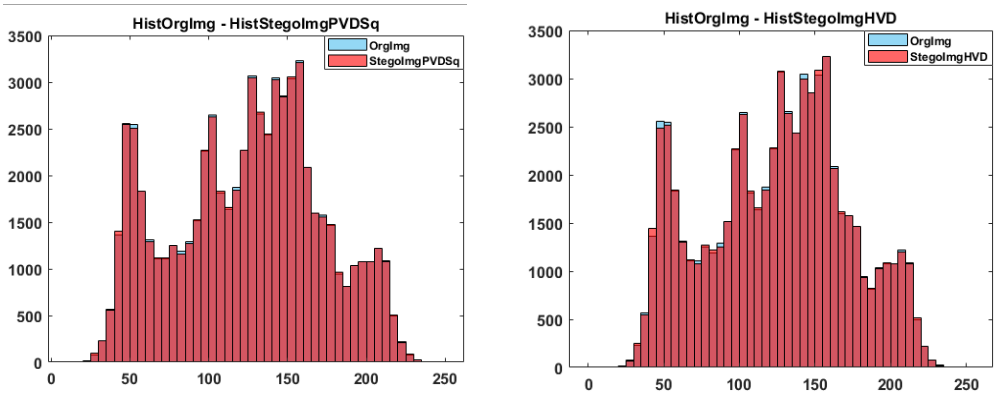
This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

TABLE III
THE CAPACITY AND SIMILARITY ANALYSIS IMPLEMENTED FOR THE TWO RANGE TABLES, (8,8,16,32,64,128) AND (2,2,4,4,4,8,8,16,16,32,32,64,64)

Image		Range Table (8,8,16,32,64,128)		Range Table (2,2,4,4,4,8,8,16,16,32,32,64,64)	
		RLBHVD	PVD_Sq [32]	RLBHVD	PVD_Sq [32]
Lena	Capacity (BPP)	2.11	1.60	1.08	0.84
	PSNR	35.54	39.58	42.57	46.36
	SSIM	0.9837	0.9577	0.9950	0.9838
Baboon	Capacity (BPP)	2.19	1.61	1.34	0.96
	PSNR	35.36	40.78	41.75	47.15
	SSIM	0.9898	0.9703	0.9939	0.9897
Airplane	Capacity (BPP)	2.13	1.59	1.12	0.80
	PSNR	35.06	40.36	41.79	47.23
	SSIM	0.9831	0.9576	0.9942	0.9833
Boat	Capacity (BPP)	2.19	1.63	1.26	0.93
	PSNR	34.08	39.12	40.62	45.62
	SSIM	0.9871	0.9657	0.9944	0.9871
House	Capacity (BPP)	2.05	1.54	1.00	0.70
	PSNR	37.65	42.06	45.33	49.99
	SSIM	0.9829	0.9597	0.9958	0.9830
Pepper	Capacity (BPP)	2.11	1.60	1.19	0.89
	PSNR	35.8	40.18	42.47	46.67
	SSIM	0.9863	0.9664	0.9941	0.9862



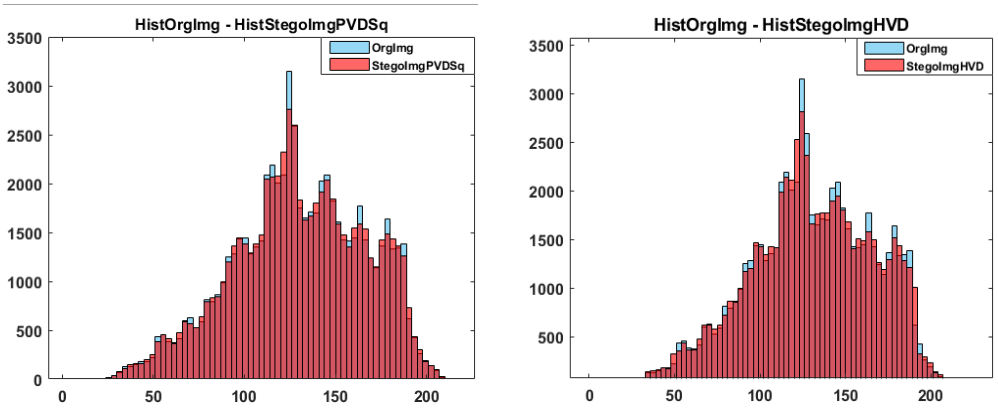
(a) Lena (8,8,16,32,64,128)



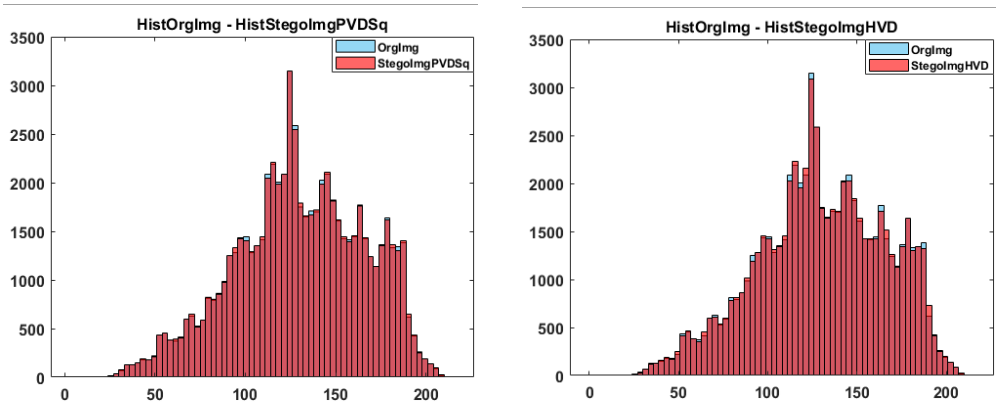
(b) Lena (2,2,4,4,4,8,8,16,16,32,32,64,64)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

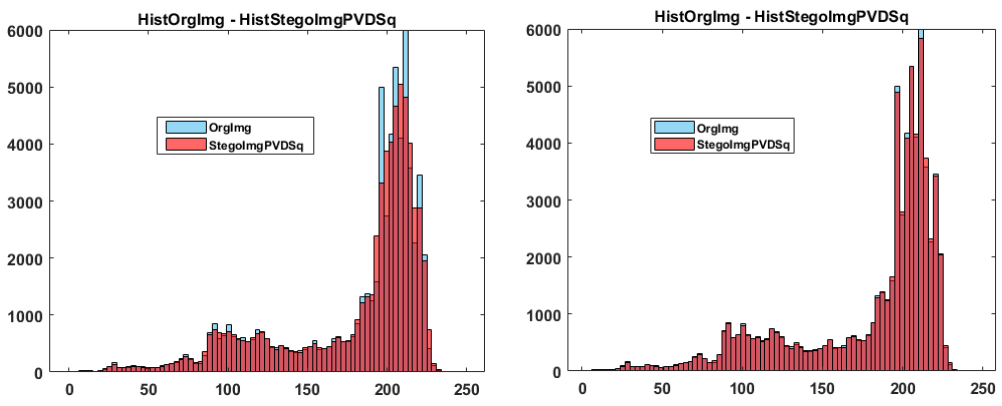
This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857



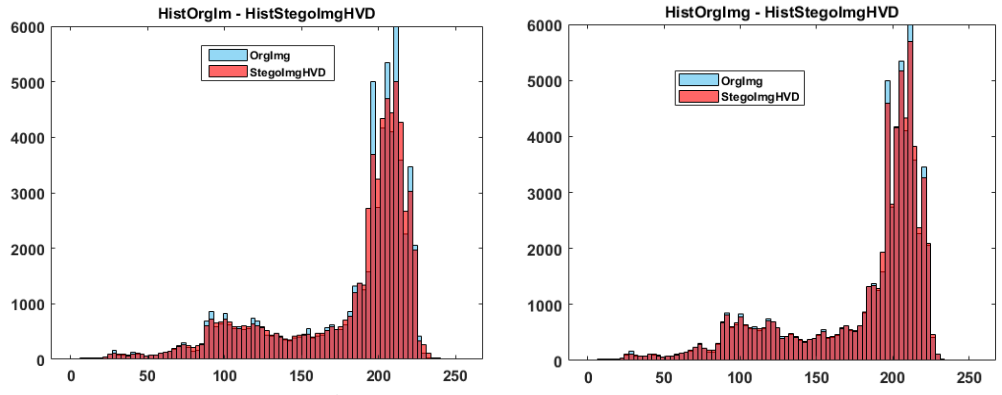
(c) Baboon (8,8,16,32,64,128)



(d) Baboon (2,2,4,4,4,8,8,16,16,32,32,64,64)



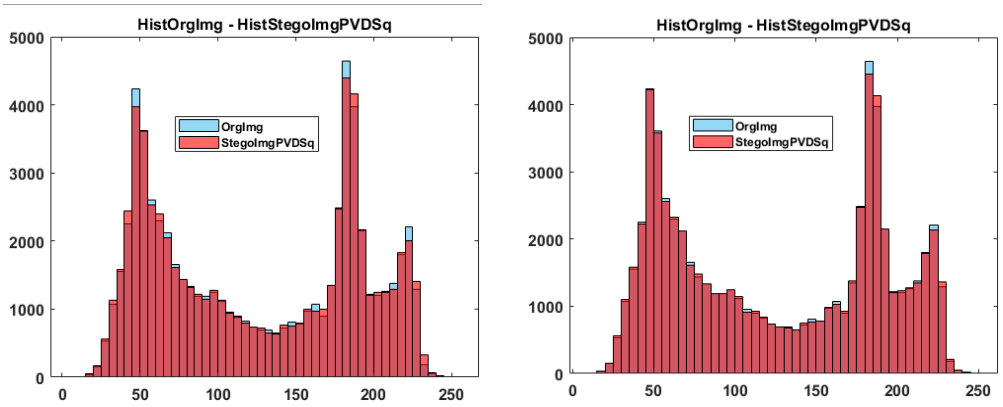
(e) Airplane (8,8,16,32,64,128)



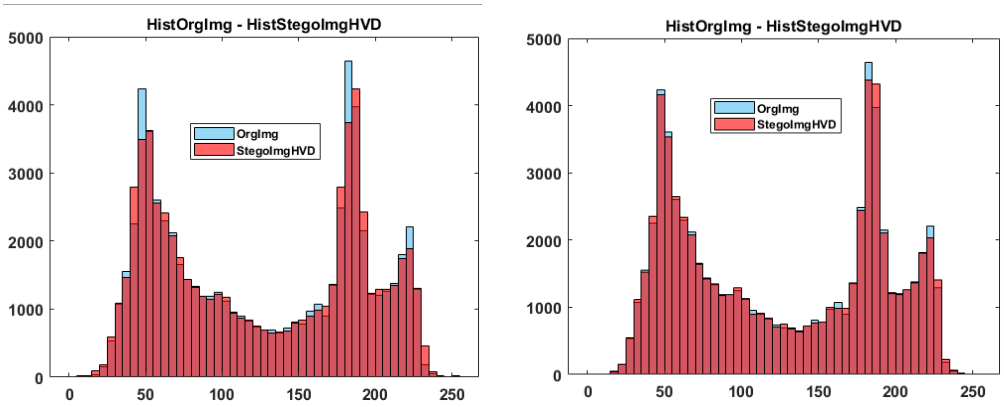
(f) Airplane (2,2,4,4,4,8,8,16,16,32,32,64,64)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

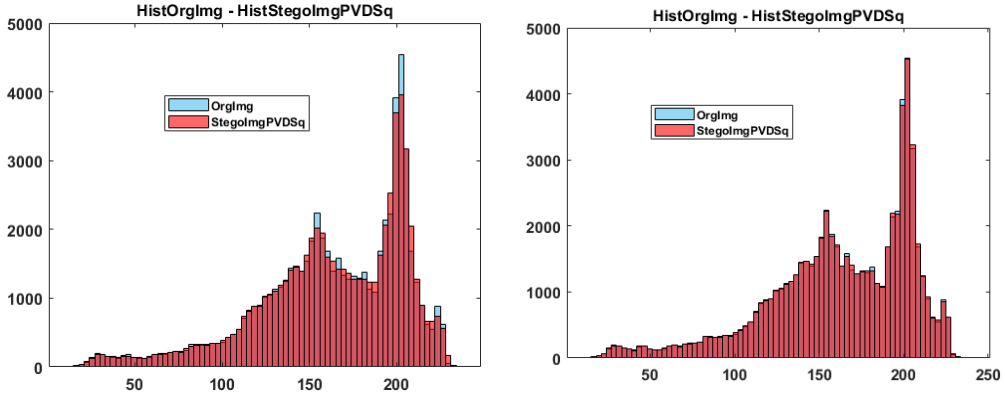
This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857



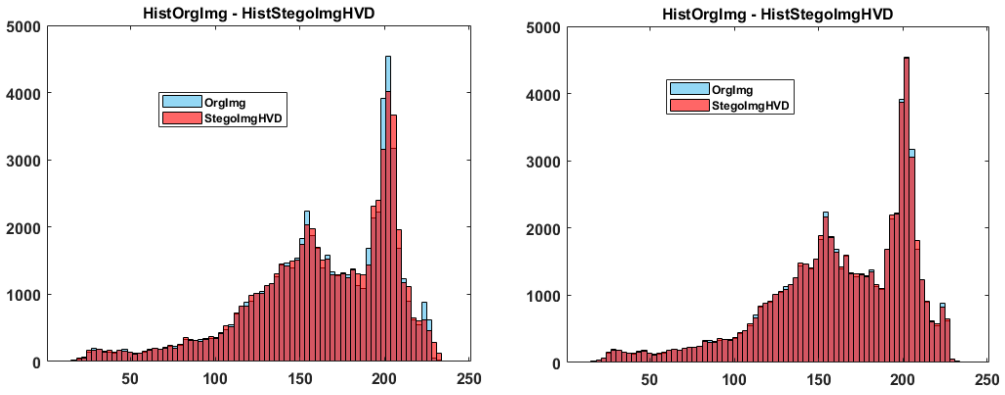
(g) Sailboat (8,8,16,32,64,128)



(h) Sailboat (2,2,4,4,4,8,8,16,16,32,32,64,64)



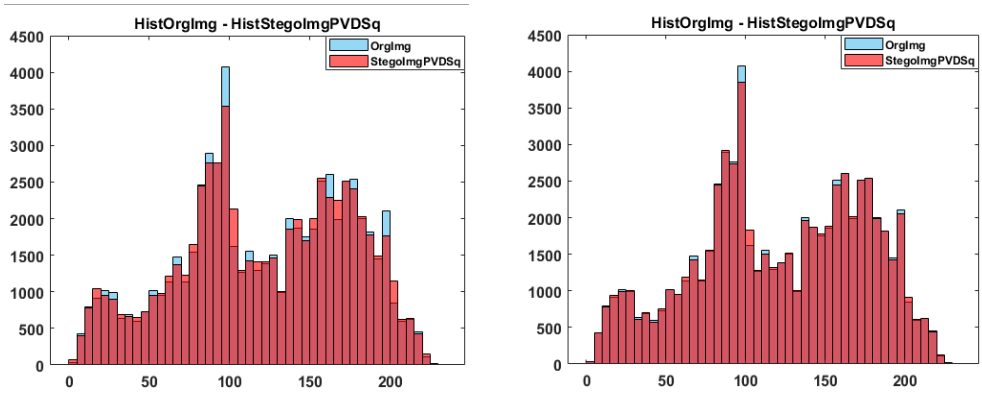
(i) House (8,8,16,32,64,128)



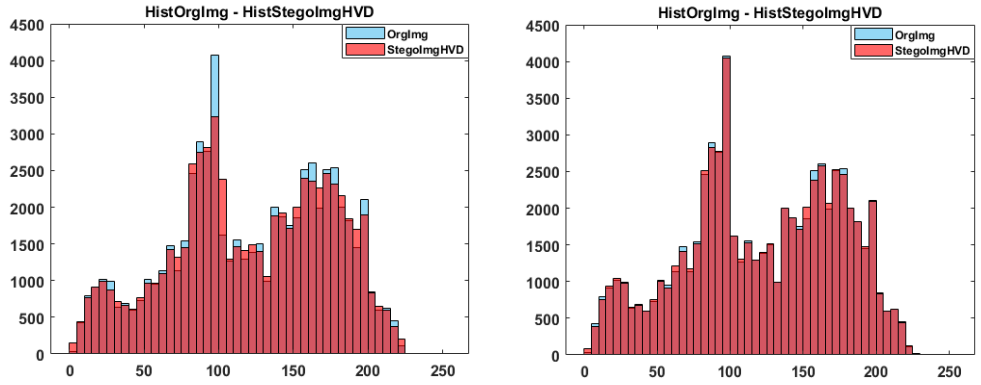
(j) House (2,2,4,4,4,8,8,16,16,32,32,64,64)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857



(k) Peppers (8,8,16,32,64,128)



(l) Peppers (2,2,4,4,4,8,8,16,16,32,32,64,64)

FIGURE 9. Histogram comparison of the cover images (Lena, Baboon, Airplane, Sailboat, House, Peppers) and their corresponding stego-images for the range tables (8,8,16,32,64,128) and (2,2,4,4,4,8,8,16,16,32,32,64,64).

The data is concealed using these eight difference values. Regarding two separate range tables, there are two types. Type 1 (T1) employs range table 1 and 3-bit modified LSB substitution. Type 2 (T2) employs range table 2 and a 4-bit modified LSB replacement. Another work we compared is the method called Tri-way Pixel-Value Differencing (TPVD) proposed by Chang et al [3]. TPVD takes into consideration three separate directional edges to build the tri-way pixel-value differencing system to increase the concealing capacity of the original PVD approach, which only refers to one direction. In addition, an ideal method of choosing the reference point and adaptive criteria is described to lessen the quality distortion of the stego-image caused by setting a bigger embedding capacity. The last of the studies we compared is the adaptive LSB substitution steganography technique based on PVD (ALSBPVD) presented by Mandal et al [48]. ALSBPVD partitions the grayscale image in 3×3 or 3×3 plus 2×2 pixel blocks. One pixel in a block is known as the reference pixel, where 4 LSBs are changed. The difference values between each neighboring pixel and the center pixel are then computed. The surrounding pixels receive adaptive LSB replacement based on these difference values.

The aforementioned techniques produce high embedding capacities, as shown in Table IV. High embedding capacity, on the other hand, carries the burden of more image distortion, which results in greater divergence between the original image and the stegoimage. 8D_PVD_T1 has an average embedding capacity of 3.36 BPP, whereas 8D_PVD_T2 has an average embedding capacity of 4.15 BPP. The average PSNR for 8D_PVD_T1 is 17.96 dB, whereas the average PSNR for 8D_PVD_T2 is 18.37 dB. The embedding capabilities of TPVD and ALSBPVD are 2.36 BPP and 4.26 BPP, respectively, while having low PSNR values of 25.98 dB and 11.07 dB, respectively. However, RLBHVD obtains a high average PSNR value of 35.58 dB and an average embedding capacity of 2.13 BPP.

The security performance analysis of the proposed method is done by performing the RS steganalysis test suggested by Fridrich et al. [20]. The RS steganalysis technique divides each stego-pixel into one of three-pixel groups: the regular group (v or R_{-M}), the single group (S_M or S_{-M}), and the unusable group. When the relative number of R_M equals that of R_{-M}, i.e., ($R_M \cong R_{-M}$), and the relative number of S_M equals that of S_{-M}, i.e., ($S_M \cong S_{-M}$), the stegoimage passes the RS detector [49]. If not, the stego-image is recognized as a suspicious image that might contain secret data. With the suggested masks $M = [0\ 1\ 1\ 0]$ and $-M = [0\ -1\ -1\ 0]$, we computed the detection results in terms of the percentage of concealing capacity about the percentage of the regular and singular pixel groups for the proposed scheme verification. As presented in Table V, the proposed method satisfies the two conditions required to resist the RS detector attack.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

TABLE IV
THE CAPACITY AND SIMILARITY ANALYSIS IMPLEMENTED FOR THE STATE OF THE ART METHODS

Image		8D_PVD_T1 [47]	8D_PVD_T2 [47]	TPVD [3]	ALSBPVD [48]
Lena	Capacity (BPP)	3.33	4.02	2.36	4.32
	PSNR	18.61	19.04	25.78	11.61
	SSIM	0.32	0.33	0.83	0.04
Baboon	Capacity (BPP)	3.30	3.96	2.46	4.29
	PSNR	19.35	19.54	25.26	12.52
	SSIM	0.40	0.41	0.68	0.04
Airplane	Capacity (BPP)	3.43	4.36	2.37	4.12
	PSNR	16.55	17.17	25.35	9.98
	SSIM	0.28	0.29	0.82	0.04
Boat	Capacity (BPP)	3.38	4.21	2.43	4.31
	PSNR	17.50	18.00	23.98	10.17
	SSIM	0.38	0.39	0.78	0.04
House	Capacity (BPP)	3.38	4.22	2.33	4.18
	PSNR	17.49	17.95	29.87	11.06
	SSIM	0.27	0.27	0.88	0.03
Pepper	Capacity (BPP)	3.35	4.12	2.37	4.33
	PSNR	18.29	18.53	25.62	11.09
	SSIM	0.33	0.33	0.77	0.03

TABLE V
THE RS STEGANALYSIS IMPLEMENTED FOR THE TWO RANGE TABLES, (8,8,16,32,64,128) AND (2,2,4,4,4,8,8,16,16,32,32,64,64)

Image		Range Table (8,8,16,32,64,128)		Range Table (2,2,4,4,4,8,8,16,16,32,32,64,64)	
		RLBHVD	PVD_Sq [32]	RLBHVD	PVD_Sq [32]
Lena	R_M	0.3605	0.3953	0.3659	0.3944
	R_{-M}	0.4378	0.3964	0.4637	0.3961
	S_M	0.3028	0.2549	0.2713	0.2652
	S_{-M}	0.2370	0.2554	0.1970	0.2590
Baboon	R_M	0.3623	0.3785	0.3609	0.3752
	R_{-M}	0.4000	0.3742	0.4015	0.3708
	S_M	0.3370	0.3114	0.3295	0.3099
	S_{-M}	0.3011	0.3213	0.2893	0.3129
Airplane	R_M	0.3865	0.4115	0.3805	0.4039
	R_{-M}	0.4289	0.4003	0.4661	0.4065
	S_M	0.3118	0.2792	0.3083	0.2834
	S_{-M}	0.2726	0.2862	0.2358	0.2861
Boat	R_M	0.3688	0.3867	0.3739	0.3864
	R_{-M}	0.4051	0.3863	0.4242	0.3896
	S_M	0.3199	0.2986	0.3133	0.3004
	S_{-M}	0.2884	0.2978	0.2744	0.3046
House	R_M	0.3617	0.3860	0.3535	0.3846
	R_{-M}	0.4282	0.3876	0.5023	0.3841
	S_M	0.2845	0.2624	0.2582	0.2577
	S_{-M}	0.2282	0.2649	0.1700	0.2646
Pepper	R_M	0.3629	0.3904	0.3627	0.3856
	R_{-M}	0.4085	0.3812	0.4285	0.3929
	S_M	0.3198	0.2912	0.3063	0.2958
	S_{-M}	0.2793	0.2957	0.2573	0.2905

VI. CONCLUSION

The field of Hexagonal-pixel (Hexel)-based Image Processing (HIP) has received limited attention, primarily attributed to the absence of crucial hardware, mathematical frameworks, and software infrastructure capable of effectively processing hexagonal pixels (hexels). However, HIP must undergo a thorough investigation to ascertain its potential in alleviating the data size challenges often faced and subsequently reducing processing time. Image steganography is the method of

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

concealing hidden data in a digital image surreptitiously. Even though steganography has significantly improved in SIP, there has been no attempt to include it in the HIP. To our knowledge, no steganography technique for the HIP domain has yet been proposed. This study is the first of its type in this field. This paper introduces Reversible Logic-Based Hexel Value Differencing (RLBHVD) in the HIP domain, an S-D data concealing technique. The performance of a data-hiding method hinges on two key factors: the capacity to conceal data within the content and the extent of alteration introduced between the original version and the newly produced material through data-hiding techniques. These elements play a critical role in evaluating the efficacy and suitability of a data-hiding approach. Based on the conducted simulations, it was observed that steganography in the HIP domain surpasses steganography in the SIP domain based on both data concealment capacity and the level of alteration introduced in the content post-data hiding. These findings underscore the superior performance of HIP-based steganography techniques.

Future research endeavors should focus on refining and expanding HIP-compatible steganography methods, drawing insights from the present study, which pioneers steganography techniques in the HIP domain, and leveraging the established infrastructure to facilitate advancements in this area.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

Data sharing does not apply to this article, as no new datasets were generated or analyzed during the current study.

REFERENCES

[1] R.-M. Chao, H.-C. Wu, C.-C. Lee, and Y.-P. Chu, "A Novel Image Data Hiding Scheme with Diamond Encoding," *EURASIP Journal on Information Security*, vol. 2009, no. 1, p. 658047, 2009, doi: 10.1186/1687-417X-2009-658047.

[2] D. Lerch-Hostalot and D. Megías, "LSB matching steganalysis based on patterns of pixel differences and random embedding," *Computers & Security*, vol. 32, pp. 192–206, Feb. 2013, doi: 10.1016/j.cose.2012.11.005.

[3] K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing," *Journal of Multimedia*, vol. 3, no. 2, pp. 37–44, Jun. 2008, doi: 10.4304/jmm.3.2.37-44.

[4] L. Ke and Z. Yin, "On the security and robustness of 'Keyless dynamic optimal multi-bit image steganography using energetic pixels,'" *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 3997–4005, Jan. 2021, doi: 10.1007/s11042-020-09807-4.

[5] Xinpeng Zhang and Shuozhong Wang, "Steganography using multiple-base notational system and human vision sensitivity," *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 67–70, Jan. 2005, doi: 10.1109/LSP.2004.838214.

[6] X. Wang and J. Yang, "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient," *Information Sciences*, vol. 569, pp. 217–240, Aug. 2021, doi: 10.1016/j.ins.2021.04.013.

[7] Q. Li *et al.*, "Image steganography based on style transfer and quaternion exponent moments," *Applied Soft Computing*, vol. 110, 2021, doi: 10.1016/j.asoc.2021.107618.

[8] R. Roy, S. Changder, A. Sarkar, and N. C. Debnath, "Evaluating image steganography techniques: Future research challenges," in *2013 International Conference on Computing, Management and Telecommunications, ComManTel 2013*, 2013, pp. 309–314. doi: 10.1109/ComManTel.2013.6482411.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[10] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in *Media Forensics and Security II*, 2010, vol. 7541, p. 754105. doi: 10.1117/12.838002.

[11] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 111–119, Mar. 2006, doi: 10.1109/TIFS.2005.863485.

[12] T. Cevik, M. Fettahoglu, N. Cevik, and S. Yilmaz, "FTSH: a framework for transition from square image processing to hexagonal image processing," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7021–7048, 2020, doi: 10.1007/s11042-019-08487-z.

[13] S. Coleman, B. Scotney, and B. Gardiner, "Processing hexagonal images in a virtual environment," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5716 LNCS, pp. 920–928. doi: 10.1007/978-3-642-04146-4_98.

[14] J. D. Allen, "Perfect reconstruction filter banks for the hexagon grid," in *2005 Fifth International Conference on Information, Communications and Signal Processing*, 2005, vol. 2005, pp. 73–76. doi: 10.1109/icics.2005.1689007.

[15] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018, doi: 10.1007/s11042-017-5308-3.

[16] T. Morkel, M. S. Olivier, and J. H. . Eloff, "An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, 2005, vol. 83, no. July, pp. 51–107. [Online]. Available: http://martinolivier.com/open/stegoverview.pdf

[17] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Information Sciences*, vol. 553, pp. 19–30, Apr. 2021, doi: 10.1016/j.ins.2020.12.002.

[18] Q. Li, X. Wang, X. Wang, and Y. Shi, "CCCIH: Content-consistency Coverless Information Hiding Method Based on Generative Models," *Neural Processing Letters*, vol. 53, no. 6, pp. 4037–4046, Dec. 2021, doi: 10.1007/s11063-021-10582-y.

[19] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13–14, no. C, pp. 95–113, Nov. 2014, doi: 10.1016/j.cosrev.2014.09.001.

[20] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedings of the 2001 workshop on Multimedia and security new challenges - MM&Sec '01*, 2001, no. II, p. 27. doi: 10.1145/1232454.1232466.

[21] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, Jun. 2005, doi: 10.1109/LSP.2005.847889.

[22] J. Fridrich, M. Goljan, and Rui Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, 2001, doi: 10.1109/93.959097.

[23] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive-noise modelable information hiding," in *In Proceedings of SPIE: Security and watermarking of multimedia contents*, Jun. 2003, pp. 131–142. doi: 10.1117/12.476813.

[24] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, Mar. 2004, doi: 10.1016/j.patcog.2003.08.007.

[25] T. Sharp, "An Implementation of Key-Based Digital Signal Steganography," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2137, 2001, pp. 13–26. doi: 10.1007/3-540-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857

45496-9_2.
[26] A. D. Ker, "Improved Detection of LSB Steganography in Grayscale Images," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3200, 2004, pp. 97–115. doi: 10.1007/978-3-540-30114-1_8.
[27] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, May 2006, doi: 10.1109/LSP.2006.870357.
[28] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781–783, Nov. 2006, doi: 10.1109/LCOMM.2006.060863.
[29] T. D. Kieu and C.-C. Chang, "A steganographic scheme by fully exploiting modification directions," *Expert Systems with Applications*, vol. 38, no. 8, pp. 10648–10657, Aug. 2011, doi: 10.1016/j.eswa.2011.02.122.
[30] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, Jun. 2003, doi: 10.1016/S0167-8655(02)00402-6.
[31] H.-W. Tseng and H.-S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," *Journal of Applied Mathematics*, vol. 2013, pp. 1–8, 2013, doi: 10.1155/2013/189706.
[32] S.-Y. Shen and L.-H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Computers & Security*, vol. 48, pp. 131–141, Feb. 2015, doi: 10.1016/j.cose.2014.07.008.
[33] A. Pradhan, K. R. Sekhar, and G. Swain, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks," *Security and Communication Networks*, vol. 2017, 2017, doi: 10.1155/2017/1924618.
[34] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K.-H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image Communication*, vol. 50, pp. 44–57, Feb. 2017, doi: 10.1016/j.image.2016.10.005.
[35] W. Luo, F. Huang, and J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," *Multimedia Tools and Applications*, vol. 52, no. 2–3, pp. 407–430, Apr. 2011, doi: 10.1007/s11042-009-0440-3.
[36] G. Swain and S. K. Lenka, "Steganography using two sided, three sided, and four sided side match methods," *CSI Transactions on ICT*, vol. 1, no. 2, pp. 127–133, Jun. 2013, doi: 10.1007/s40012-013-0015-3.
[37] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142–172, 2011, doi: 10.1201/b12697-11.
[38] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Varied PVD+LSB evading detection programs to spatial domain in data embedding systems," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1635–1643, Oct. 2010, doi: 10.1016/j.jss.2010.03.081.
[39] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, p. 108908, May 2023, doi: 10.1016/j.sigpro.2022.108908.
[40] P. N. Andono and D. R. I. M. Setiadi, "Quantization selection based on characteristic of cover image for PVD Steganography to optimize imperceptibility and capacity," *Multimedia Tools and Applications*, vol. 82, no. 3, pp. 3561–3580, Jan. 2023, doi: 10.1007/s11042-022-13393-y.
[41] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Graded fuzzy edge detection for imperceptibility optimization of image steganography," *The Imaging Science Journal*, pp. 1–13, Jun. 2023, doi: 10.1080/13682199.2023.2219880.
[42] S. Rustad, I. M. S. De Rosal, P. N. Andono, A. Syukur, and Purwanto, "Optimization of Cross Diagonal Pixel Value Differencing and Modulus Function Steganography Using Edge Area Block Patterns," *Cybernetics and Information Technologies*, vol. 22, no. 2, pp. 145–159, Jun. 2022, doi: 10.2478/cait-2022-0022.
[43] R. P. Feynman, "Quantum mechanical computers," *Foundations of Physics*, vol. 16, no. 6, pp. 507–531, Jun. 1986, doi: 10.1007/BF01886518.
[44] University of Southern California, "SIPI Image Database." http://sipi.usc.edu/services/database/Database.html (accessed Dec. 20, 2022).
[45] Y. Rubner, C. Tomasi, and L. J. Guibas, "Earth mover's distance as a metric for image retrieval," *International Journal of Computer Vision*, vol. 40, no. 2, pp. 99–121, 2000, doi: 10.1023/A:1026543900054.
[46] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, doi: 10.1007/s11042-020-10035-z.
[47] G. Swain, "Digital Image Steganography Using Eight-Directional PVD against RS Analysis and PDH Analysis," *Advances in Multimedia*, vol. 2018, pp. 1–13, Sep. 2018, doi: 10.1155/2018/4847098.
[48] B. Mandal, A. Pradhan, and G. Swain, "Adaptive LSB substitution Steganography technique based on PVD," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Apr. 2019, pp. 459–464. doi: 10.1109/ICOEI.2019.8862579.
[49] A. Malik, S. Singh, and R. Kumar, "Recovery based high capacity reversible data hiding scheme using even-odd embedding," *Multimedia Tools and Applications*, vol. 77, no. 12, pp. 15803–15827, Jun. 2018, doi: 10.1007/s11042-017-5156-1.



TANER CEVIK received the B.Sc. degree in computer engineering from Istanbul Technical University, Istanbul in 2001, and completed Ph.D. at Istanbul University in 2012. He joined the Department of Computer Engineering at Istanbul Arel University in 2023 and continues to work as Professor. His research interests are Image Processing, Machine Learning and Wireless Communications.



NAZIFE CEVIK obtained the Ph.D. degree from Istanbul University in 2015. She joined the Computer Engineering Department at Istanbul Arel University in 2015 and continues to work as an Associate Professor. Her research interests are Image Processing, Machine Learning and Bioinformatics.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3326857



JAWAD RASHEED (M'19) received a B.S. degree in telecommunication engineering from the National University of Computer and Emerging Sciences, Pakistan. He then moved to Turkey, where he earned an M.S. degree in electrical and electronics engineering and a Ph.D. degree in computer engineering. He was a gold medalist and awarded the Academic Excellence Award for securing straight A's in O' Level exams held by Cambridge University. Later, he also received a prestigious Doctorate and Research Scholarship for his Ph.D. studies (for three years). Dr. Rasheed is currently working as Senior Researcher at Deep Learning and Medical Image Analysis Laboratory, Bogazici University, Turkey, a Research Fellow at Istanbul Nisantasi University and Istanbul Sabahattin Zaim University, Turkey.

He is the author/co-author of more than 50 articles published in well-reputed journals and highly ranked conferences. He serves as guest/lead-guest/topic editor for special issues at the Symmetry, Mathematics, Healthcare, Applied Sciences, Electronics, Healthcare, and Journal of Sensor and Actuator Networks. Recently, he served as a book editor for Springer Lecture Notes on Data Engineering and Communications Technologies (Forthcoming Networks and Sustainability in the IoT Era). In addition, he is the general chair of IEEE ICAIoT and IEEE FoNeS-AIoT and chairs the technical program committee of Springer FoNeS-IoT 2021. His research interests include artificial intelligence and image processing. pattern recognition, IoT, and data analytics.



TUNC ASUROGLU obtained received the B.S. degree in computer engineering from the TOBB University of Economics and Technology, Turkey, in 2013, and the M.S. and Ph.D. degrees in computer engineering from Başkent University, Turkey, in 2015 and 2020, respectively. He was an Assistant Professor with the Department of Computer Engineering, Başkent University. He was also a Guest Researcher with the Faculty of Computer Sciences, Østfold University College, Norway. He worked on many international projects related to health informatics. He is currently a Postdoctoral Research Fellow with the Faculty of Medicine and Health Technology, Tampere University, Tampere, Finland. His research interests include the applications of computational intelligence in health informatics and wearable sensor systems.



SHTWAI ALSUBAI received the bachelor's degree in information system from King Saud University, Saudi Arabia, in 2008, the master's degree in computer science from CLU, USA, in 2011, and the Ph.D. degree from The University of Sheffield, U.K., in 2018. He is currently an Assistant Professor of computer science at Prince Sattam bin Abdulaziz University. His research interests include XML, XML query processing, XML query optimization, machine learning, and natural language processing.



MEHMET TURAN received his diploma degree from RWTH Aachen University, Germany in 2012 and his PhD from ETH Zurich, Switzerland in 2018. Between 2013-2014, he was a research scientist at UCLA, USA. Between 2018-2019, he was a postdoctoral fellow at Max Planck Institute for Intelligent Systems. In October 2019, he joined the Institute of Biomedical Engineering, Bogazici University after receiving the TUBITAK 2232 International Outstanding Researchers Fellowship. His research interests include the development of multimodal fusion algorithms to combine information from multiple imaging modalities, family and patient histories to make more accurate diagnostic, prognostic and therapeutic determinations.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/