A NOVEL APPROACH FOR NON-DESTRUCTIVE STEGANOGRAPHY BY PREDETERMINATION

Valentin Atanasov, Daniel Denev, Tsvetoslav Tsankov*

Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Shumen Bulgaria

* Corresponding Author, e-mail: v.atanasov@shu.bg

Abstract: This paper presents a non-destructive steganography method that constructs static images based on a diffusion-stable approaches with hex description of hidden data. Unlike traditional approaches that embed data into existing images – altering them irreversibly – this method preserves the integrity of the visual carrier. Steganography relies on human visual limitations to conceal information, and many existing techniques (e.g., LSB, transform-based, fractal, RGB methods) modify image data. These can be grouped into two types: altering digital data and overlaying templates. In contrast, our approach generates a new image from the hex input and PyTorch model with diffusion transformers. This approach could ensure secure, reversible information hiding suitable for modern confidentiality needs.

Key words: hiding data approach, image, information, non-destructive steganography, diffusion transformers.

1. INTRODUCTION

The volume of digital information—including data processing, storage, and global usage in modern society—has grown exponentially, increasing 60-fold over 13 years to reach 120 billion terabytes by 2023. Projections estimate it will exceed 180 billion terabytes by the end of 2025. This outlines its level as extremely high and with a sustainable upward trend [1]. In the stage of the Fourth Industrial Revolution 4.0, a certain opportunity arises for humans to implement their own strategies with the capabilities of machines [2] to achieve the most effective way of data processing.

In this aspect, the presence of approaches in which the exchange of this data should be reliable, and the data protected, sets requirements for the construction of mechanisms that ensure this protection. One sustainable and commonly applied approach is steganography. This form of data hiding has its development as a result of a number of objective circumstances arising from the security domain. This led to the development of a number of methods for "embedding" information using digital images.

Scientists have built the logic of confidentiality in the transmission of digital data through images, relying on the physiological characteristics or more precisely, the limitations of the human visual organ with a characteristic spectrum of visible light

absorption, or in other words – the sensitivity of the eye to wavelength. Without considering the physiological prerequisites in detail, the argument will be presented that with normal colour vision the human eye is able to distinguish the change in wavelength of the visible spectrum with a step bordering on 1 nm [5, 6]. This provides an opportunity to change (manipulate) the colour parameters of a given image with a range guaranteed by at least 1 bit, without this change being noticed by human vision. This approach with the change of the digital description of an existing image is widely used, ensuring the "hiding" of purposefully embedded data.

Based on existing approaches [3, 4, 7-13] for hiding messages in an existing static image, a set of methods can be formed, which are in the field of applications listed below:

- Least significant bit (LSB) method;
- Transformation domain method;
- Colour palette method;
- Blue noise steganography method;
- Histogram-based steganography method;
- Fractal steganography method;
- Surface encoding method;
- Block-based steganography method;
- RGB channel steganography method;
- Reverse Steganography;
- Image Masking Steganography;
- Path-Based Steganography.

In addition to the methods mentioned above, the use of encryption algorithms in hiding data in images is widely used, among which are approaches based on the Shannon algorithm. There is the practice of hiding data in technologies such as blockchain, referring to the act of embedding hidden data within transactions or other data structures of a blockchain [14]. For the above methods, their main characteristic can be formed. This key characteristic creates two main categories in the considered steganography approaches [1, 3, 15]:

- Changing the digitally represented data;
- Superimposing data or templates on the carrier graphic file.

Based on the application areas, the following summary of the data hiding methods listed above can be made using several key indicators (table 1.) [16]:

Table 1. Summary for areas of the steganography application

Method	***Range***	***Area***	***Characteristics***
Least Significant Bit	*Wide*	*Spatial Domain*	*Easy to implement. Vulnerable to compression*
Transformation Domain	*Wide*	*Frequency Domain (DCT, DWT)*	*More resistant to processing*
Colour Palette	*Moderate*	*Color Models/Palettes*	*Suitable for palleted images.*
Blue Noise	*Minimal*	*Noise Techniques*	*Uses noise patterns to make detection*
Histogram-Based	*Moderate*	*Image Analysis/ Distribution*	*Uses statistical properties, suitable for detection and protection.*

Fractal	*Minimal*	*Fractals and Self-Similarity*	*Uses fractal structures*
Surface Encoding	*Minimal*	*3D/Vector Surfaces*	*Uses 3D models*
Block-Based Steganography	*Moderate*	*Block Separation (Spatial/Frequency)*	*Used in combination with other methods*
RGB Channel	*Wide*	*Color Channels (R, G, B)*	*Uses separate color channels*
Reverse	*Minimal*	*Analysis/Detection via Inverse Techniques*	*For discovering hidden data*
Image Masking	*Moderate*	*Visual Cloaking*	*For hiding in opaque areas*
Path-Based	*Minimal*	*Contour or Trajectory Embedding*	*Focus on image routes.*

As one of the most widely used methods, LSB has been the subject of numerous studies. In [17], this method is presented with strong visual and statistical analysis, along with positive results from its application. In another study, related to this topic, four major statistical properties describing the degree of similarity between two images are calculated [18].

All of the above approaches could form the following conclusion – *Destructiveness of the original image*. This is due to the fundamental principle underlying the above methods – *Embedding semantic data into an existing image data*.

This publication proposes another principle for hiding data – building a static image using a hex input description of the data. This is a non-destructive approach by its nature.

The emergence of open-source machine learning frameworks such as PyTorch presents significant opportunities in steganography, particularly in the development of non-destructive information hiding techniques. Classical steganography techniques often rely on and refer to the basics of modifying the carrier data, which can lead to loss of quality or easy disclosure of the hidden text content in them. Contemporary steganographic research emphasizes predefined methods that facilitate the embedding of information with minimal alterations to the original data. In research [5], author considers the measurement of the wavelength discrimination threshold across the visible spectrum, which optimizes the predetermination processes in steganography. Another researcher [15] focuses on steganography approaches through data hiding, which supports the analysis of steganographic methods and reduce the cognitive load of researchers. In another study [3], the techniques used for hidden information encoding is analysed.

Our current study builds upon previous research in steganography by proposing an advanced and rarely explored non-destructive steganographic method based on diffusion-stable approaches.

2. CONCEPTUAL MODEL

The main idea of the conceptual model is to create a source using a hexadecimal description of data, which will be the basis for building a two-dimensional image. This

hexadecimal description represents a static character string forming a message, and existing encoding standards such as Unicode, ASCII, or ISO/IEC 8859-9:1999 can be used. The mentioned description will be considered as part of the overall description of the image. It is worth noting that this approach requires a mechanism for direct byte-level control, which is currently not supported by AI generative models such as DALL·E, Stable Diffusion, and Midjourney in their direct implementation.

Based on certain standards for lossless compression graphic file formats - for example Portable Network Graphics (PNG) [19, 20], the IDAT (Image Data) part can be considered as the target, which is part of the structure of this type of graphic file containing the actual image data. In this paper, the algorithms for compression and decompression of the data stream constructed from all IDAT file parts will not be presented, as they are currently standardized and widely applicable. The concept of the proposed approach requires the presence of several processes, through which they should cover all stages of the construction of the two-dimensional image. Figure 1 shows the conceptual logic of the model for non-destructive construction of an image based on a hex description. In the conceptual model presented in Figure 1, one of its key components is the image generator, based on generative machines such as PyTorch model with diffusion transformers.

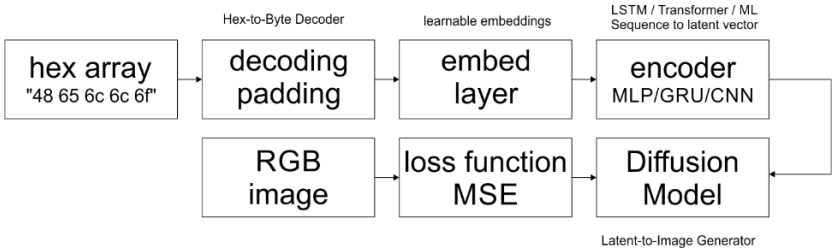

Figure 1. Conceptual model of non-destructive image construction based on hex description input for PyTorch model with diffusion transformers

Below is the short description of the proposed model.

Phase 1*(Hex input)*:
Hex-to-Byte Input (Representation of hex string)
Example: "48656c6c6f" → b"Hello"
Every 2 hex characters = 1 byte
Output: 1D array of bytes → [72, 101, 108, 108, 111]
Phase 2*(Byte Embedding Layer)**:***
Each byte number (0–255) is inserted into an embedding table → 256 x D (e.g. D=128)
Converts a sequence of bytes into a vector sequence
Phase 3(*Aggregator / Encoder*)
Collects the sequence into a latent vector via Transformer encoder
Output: Vector z of fixed length
Phase 4*(Latent-to-Image Generator*)
Generates an image from a latent vector z via Diffusion Decoder

Phase 5*(Loss function (during training))*

MSELoss is selected as it effectively maps the difference between the generated and real images.

For better understanding, the general principle of the model is shown below (Fig. 2):

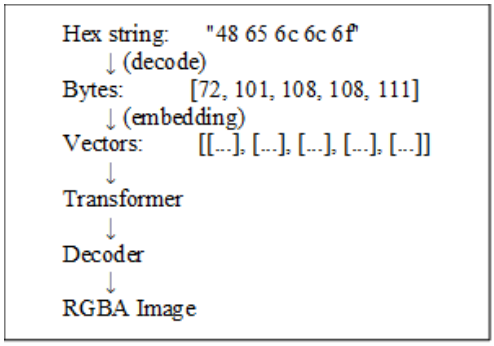

Figure 2. Basic principle of the non-destructive image construction based on hex description input for PyTorch model with diffusion transformers

It is important to note that this approach requires a model training phase, which can be achieved using a synthetic dataset (Fig. 3a, Fig. 3b).

```python
import torch
import torch.nn as nn
from torch.utils.data import Dataset, DataLoader
from torchvision.utils import save_image
import torchvision.transforms as transforms
from PIL import Image
import numpy as np

# 1. Example hex input
hex_input = "48656c6c6f20576f726c64"  # "Hello World"

# 2. Decode hex to bytes and convert to tensor
def hex_to_tensor(hex_string):
    byte_array = bytes.fromhex(hex_string)
    # Convert to a list of integers (0-255), pad or truncate to a fixed length
    max_len = 32
    byte_list = list(byte_array)[:max_len]
    if len(byte_list) < max_len:
        byte_list += [0] * (max_len - len(byte_list))  # Padding if needed
    return torch.tensor(byte_list, dtype=torch.float32) / 255.0  # Normalize to [0, 1]

input_vector = hex_to_tensor(hex_input).unsqueeze(0)  # Add batch dimension
```

Figure 3a. An example of Synthetic Database Training

```
# 3. Minimal generative model (example)
class HexToImageModel(nn.Module):
    def __init__(self, input_dim=32, img_size=64):
        super().__init__()
        self.fc = nn.Sequential(
            nn.Linear(input_dim, 256),
            nn.ReLU(),
            nn.Linear(256, img_size * img_size * 3),
            nn.Sigmoid()  # Output in range [0, 1] for pixel values
        )
        self.img_size = img_size

    def forward(self, x):
        x = self.fc(x)
        return x.view(-1, 3, self.img_size, self.img_size)  # Output RGB image

# 4. Instantiate the model and generate the image
model = HexToImageModel()
with torch.no_grad():
    output_image = model(input_vector)

# 5. Save or display the image
save_image(output_image, "generated_image.png")
```

Figure 3b. An example of Synthetic Database Training(continue)

The code shown above uses hex_input = "48656c6c6f20576f726c64" (which corresponds to "Hello World") as a reference, but in the later development phase, an actual reference will be used. In a real-world scenario, a dataset of hex strings and their corresponding images will be required for supervised learning.

Another important thing in this process is the introduction of conditional dynamic logic. The conditions of this logic are a function of external factors such as - astronomical indicators (time, day, moon phase, etc.) used as parameters, other external signals or key parameters known ONLY to both parties. This conditional logic can be built from Pre-established and Predefined Rules (PPR). These rules establish basic approaches when the model encodes or extracts the hidden data such as - reading direction (left to right, top to bottom, symbol-wise reading), coordinates of the first symbol, length of the hidden data, etc. So, under certain conditions set in the PPR, the recipient's model will apply a specific approach to reading the data, which circumstance remains unknown to third parties.

The process of extracting hidden data a separate reverse model (Decoder) needs to be trained to reconstruct the hex string from the image. The program logic for the extraction process is shown below (Fig. 4.):

Image → Encoder → Latent → Decoder → Bytes → Hex → Text

Figure 4. A program logic of the extraction process based on hex description input for PyTorch model with diffusion transformers

Due to paper length limitations, only selected functionalities and parts of the program logic will be presented. The functional diagram of decoding a hex string from an image using a Diffusion Transformer in PyTorch is presented in Figure 5.

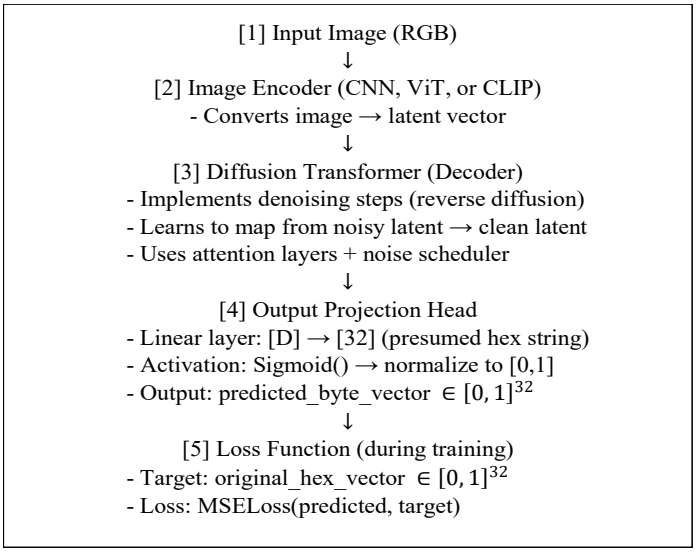

Figure 5. The functional diagram of decoding a hex string from an image using a Diffusion Transformer in PyTorch model

An example of a basic CNN encoder in PyTorch that takes an RGB image of size 3×64×64 and outputs a latent vector of size 512 is shown in Figure 6.

```python
import torch
import torch.nn as nn
import torch.nn.functional as F

class SimpleCNNEncoder(nn.Module):
    def __init__(self, latent_dim=512):
        super(SimpleCNNEncoder, self).__init__()
        self.conv1 = nn.Conv2d(3, 64, kernel_size=4, stride=2, padding=1)   # → [64, 32, 32]
        self.conv2 = nn.Conv2d(64, 128, kernel_size=4, stride=2, padding=1) # → [128, 16, 16]
        self.conv3 = nn.Conv2d(128, 256, kernel_size=4, stride=2, padding=1)# → [256, 8, 8]
        self.conv4 = nn.Conv2d(256, 512, kernel_size=4, stride=2, padding=1)# → [512, 4, 4]

        self.fc = nn.Linear(512 * 4 * 4, latent_dim)

    def forward(self, x):
        x = F.relu(self.conv1(x))  # Shape: [B, 64, 32, 32]
        x = F.relu(self.conv2(x))  # Shape: [B, 128, 16, 16]
        x = F.relu(self.conv3(x))  # Shape: [B, 256, 8, 8]
        x = F.relu(self.conv4(x))  # Shape: [B, 512, 4, 4]
        x = x.view(x.size(0), -1)  # Flatten: [B, 512 * 4 * 4]
        x = self.fc(x)             # Output: [B, latent_dim]
        return x
```

Figure 6. An example of basic CNN encoder in PyTorch

The present analysis focuses on a specific case study aimed at applying an innovative non-destructive method in the field of steganography, based on Diffusion Transformers implemented in a PyTorch model. The amount of new and innovative topics and technologies that are not addressed in the existing literature is alarming - for example, the use of non-destructive methods and approaches in the development of steganography and confidentiality of information data streams. This analysis supports the qualitative conclusions of other researchers and reveals gaps in the existing literature on non-destructive approaches in steganography.

3. CONCLUSION

The proposed non-destructive approach to create an image containing information that can be defined as confidential uses reverse logic – the generation of the image is based on hex description input for PyTorch model with diffusion transformers. One of the key advantages of this approach is the higher degree of information capacity. Compared to LSB, the proposed non-destructive approach has a theoretically 24 times greater information capacity. Another advantage is the possibility of using existing machine image generative engines, which have permanently and sustainably entered the field of digital processing. This type of generative machines enables the enhancement of the degree of automation in the process. A third advantage is the possibility of forming a set of code tables that will ensure a higher degree of confidentiality of the information carried in the image. From a security standpoint, the strength of the proposed algorithm relies on the Pre-established and Predefined Rules which are known only to both parties involved in the data exchange.

It can be concluded that, following the development of a functional program mechanism, the potential use of this non-destructive approach for concealing confidential information would expand the existing set of algorithms in this field, and on the other hand, offers higher information capacity along with enabling greater levels of automation in the process of hiding sensitive data. As a continuation of this study, the research team aims to develop a hybrid program mechanism for direct byte-level control using the technical capabilities of generative models such as DALL·E, Stable Diffusion, or Midjourney. This is necessary because, as of today, such control is not feasible [21],[22] - these generative models do not operate at the byte level but rather generate pixel values through neural networks working in latent space. After the successful implementation of this mechanism, the next step will be to accumulate a critical empirical mass of results with quantitative indicators for subsequent analysis.

ACKNOWLEDGMENTS

In this section, we would like to thank all of our loved ones for their support and motivation throughout the process of our scientific research. This publication is funded by the fund "Support for Publishing Publications in Journals with Impact Factor (IF) and Impact Rank (SJR)" of Konstantin Preslavsky University of Shumen, Republic of Bulgaria.

REFERENCES

[1] *Digital Progress and Trends Report 2023*. International Bank for Reconstruction and Development / The World Bank, 2023. ISBN: 978-1-4648-2049-6

[2] Mincheva, St. Opportunities for management with the help of a virtual voice assistant. *Proceedings of International Scientific Conference 2020*, Faculty of Artillery, Air Defense and Communication and Information Systems, 2020, pp. 446-451.

[3] Mandal, P., Mukherjee, I., Paul, G., Chatterji, B. Digital image steganography: A literature survey. *Information Sciences*, vol. 609, 2021, pp. 1451–1488. DOI: 10.1016/j.ins.2022.07.120.

[4] Subramanian, N., Al-maadeed, S., Bouridane, A. Image steganography: A review of the recent advances. *IEEE Access*, vol. 9, 2021, pp. 23409-23423. DOI: 10.1109/ACCESS.2021.3053998.

[5] Krúdy, A., Ladunga, K. Measuring wavelength discrimination threshold along the entire visible spectrum. *Polytechnica Mechanical Engineering*, vol. 45, no. 1, 2001, pp. 41–48. URL: https://pp.bme.hu/me/article/view/1406/810 (Visited on 31.05.2025).

[6] Konatham, S., Martín-Torres, J., Zorzano, M. The impact of the spectral radiation environment on the maximum absorption wavelengths of human vision and other species. *Life* (Basel), vol. 11, no. 12:1337, 2021. DOI: 10.3390/life11121337.

[7] Wu, H., Chen, L., Ching, Y. Block-based steganography method using optimal selection to reach high efficiency and capacity for palette images. *Applied Sciences*, vol. 10, no. 21, 2020. DOI: 10.3390/app10217820.

[8] Benhfid, A., Ameur, E., Taouil, Y. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 7, Sept. 2020, pp. 850-859. DOI: 10.1016/j.jksuci.2018.09.016.

[9] Bairagi, A., et al. A robust RGB channel-based image steganography technique using a secret key. *16th International Conference on Computer and Information Technology*, 2014, pp. 81-87. DOI: 10.1109/ICCITECHN.2014.6997309.

[10] Margalikas, E., Ramanauskaitė, S. Image steganography based on color palette transformation in color space. *Journal of Image and Video Processing,* vol. 82, 2019. DOI: 10.1186/s13640-019-0484-x.

[11] Hashemi, A., Payandeh, A. New steganography method based on the complex pixels. *Journal of Information Security*, vol. 3, no. 3, 2012, pp. 202-208. DOI: 10.4236/jis.2012.33025.

[12] Mandal, J. R*eversible steganography and authentication via transform encoding*. Springer Singapore, 2020. DOI: 10.1007/978-981-15-4397-5.

[13] Yadav, G., Ojha, A. Hamiltonian path-based image steganography scheme with improved imperceptibility and undetectability. *Applied Soft Computing*, vol. 73, 2018, pp. 497-507. DOI: 10.1016/j.asoc.2018.08.034.

[14] Stoyanova, V. Possibilities for using steganography methods in the quantum century. *International Scientific Journal "Security & Future"*, vol. VIII, no. 3, 2024, pp. 86-87. URL: https://stumejournals.com/journals/confsec/2024/3/86.full.pdf (Visited on 31.05.2025).

[15] Gibson, R. *Steganography: Hiding data in plain sight*. Department of Computer Science, College of Arts and Sciences, The University of North Carolina, 2015. URL: https://www.cs.unc.edu/~lin/COMP089H/LEC/steganography.pdf (Visited on 31.05.2025).

[16] Aslam, M., A., et al, Image steganography using least significant bit (LSB) - a systematic literature review, *2022 2nd International Conference on Computing and Information Technology*, 2022, DOI:10.1109/ICCIT52419.2022.9711628.

[17] Stoyanova, V. Steganography system using LSB methods. *ENTRENOVA 2018*, Conference Proceedings, September 6, 2018.

[18] Stoyanova, V., Tasheva, Zh. Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images. *Machines. Technologies. Materials*, vol. 9, no. 7, 2015, pp. 65-68.

[19] *Portable Network Graphics (PNG) Specification*, Third Edition. World Wide Web Consortium, 2025. URL: https://www.w3.org/TR/png/ (Visited on 31.05.2025).

[20] Boutell, T., et al. *PNG (Portable Network Graphics) Specification Version 1.0. Request for Comments: 2083*. URL: https://datatracker.ietf.org/doc/html/rfc2083 (Visited on 31.05.2025).

[21] Rombach, R., et al. *High-Resolution Image Synthesis with Latent Diffusion Models*, 2022, (https://arxiv.org/abs/2112.10752?utm_source=chatgpt.com) (Visited on 21.06.2025).

[22] Devesh, K. *Diffusion based Steganography Without Embedding*, 2023, https://hackmd.io/@kumar-devesh/Skps2g7k2 (Visited on 21.06.2025)

Information about the authors:

Valentin Tonev Atanasov – Associate Professor in the Department of Communication and Computer Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Bulgaria.

Daniel Rosenov Denev – Assistant Professor at the Department of Communication and Computer Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Bulgaria.

Tsvetoslav Stanislavov Tsankov – Professor in Communication and Computer Technologies Department, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Bulgaria.

Manuscript received on 03 June 2025