Enhancing CSNTSteg: Addressing Limitations In Character Spacing Normalisation And Invisibility With Different Coloured Text

Authors: Kushal D Achar *Dept. of Computer Science and Engineering*
AMC Engineering College Bengaluru, India kushphoenix2002@gmail.com

Kishal R
Dept. of Computer Science and Engineering
AMC Engineering College Bengaluru, India 11kishalr@gmail.com

Guide: Pallavi K V
Dept. of Computer Science and Engineering
AMC Engineering College Bengaluru, India pallu.gani@gmail.com

Abstract

Text steganography plays a crucial role in secure communication by concealing confidential information within text data. This research paper focuses on addressing the limitations of the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model, specifically in the areas of character spacing normalisation and invisibility with different coloured cover text. The study aims to investigate the challenges faced by CSNTSteg in effectively normalising character spacing in languages with joined letters, such as Arabic, Persian, and Jawi, and in maintaining invisibility when the cover text is in a colour different from the norm. By analysing the existing literature on text steganography and colour normalisation techniques, this research seeks to propose solutions to enhance the performance of CSNTSteg in these critical areas. Through experimental evaluations and simulations, the study will provide insights into the impact of character spacing normalisation and colour variations on the invisibility and robustness of hidden data in text steganography. The findings of this research aim to contribute to the advancement of text steganography techniques and provide recommendations for improving the effectiveness of CSNTSteg in concealing data within text data while ensuring high levels of invisibility and security.

Keywords—*Limitations, Critique, Research Paper, Methodology, Validity, Reliability*

I. INTRODUCTION

Steganography, an integral aspect of secure communication, stands as a pivotal technique in the realm of data protection. It involves the covert embedding of confidential information within seemingly innocuous data, thereby thwarting unauthorised access and ensuring the confidentiality of sensitive information [1,p.5]. The significance of steganography is underscored across diverse sectors, including governmental agencies, healthcare facilities, legal institutions, and financial organisations, where safeguarding information integrity and confidentiality is of paramount importance [1,p.2]. By concealing messages within cover media such as images [3],[4], audio files, videos, and text [5],[6], steganography offers a discreet and effective means of communication, impervious to detection by unintended recipients.Additionally, recent advancements in cross- modal steganography have introduced innovative approaches to enhancing the security and robustness of covert communication systems [2]

A. Text Steganography

Among the various forms of steganography, text steganography holds a prominent position, particularly in contexts where written communication is prevalent [1,p.5]. This method involves embedding secret messages within the structure of textual data, ensuring that the hidden information remains imperceptible to unintended readers. Text steganography techniques aim to strike a delicate balance between maximising information capacity and maintaining the invisibility of embedded data within the cover text.

B. Approaches in Text Steganography

Text steganography employs diverse approaches [5] to achieve effective concealment of information. These methodologies encompass modifying text structure, altering formatting or styling, leveraging linguistic properties, and manipulating visual appearance to seamlessly embed secret messages [1,p.5]. By harnessing these techniques, text steganography models bolster the security of communication channels and safeguard sensitive information from unauthorised access.

C. Introduction of CSNTSteg

In this landscape, the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model a promising solution emerges to tackle the issue, challenges inherent in text steganography. Particularly notable are its advancements in character spacing normalisation and maintaining invisibility with diverse coloured cover text. By building upon established steganography principles and incorporating innovative strategies, CSNTSteg aims to enhance the capacity and security of hidden data within text, thereby contributing significantly to the advancement of secure communication methodologies in the digital age.

II. LITERATURE REVIEW

The field of text steganography has witnessed significant advancements and innovations aimed at enhancing the capacity and invisibility of hidden data within textual content. Researchers have explored various techniques and models to improve the security and efficiency of text-based communication channels. This literature review provides an overview of key studies and methodologies in text steganography, highlighting the evolution of approaches to concealing information within text.

Text steganography techniques can be categorised into coverless, linguistic, and structural methods, each offering unique advantages in concealing sensitive information within textual data [1,p.1]. Coverless steganography techniques, also known as random and statistical methods, leverage the statistical characteristics of the secret message to automatically generate cover text without the need for pre-existing content [1,p.1]. These techniques rely on the linguistic features and structures of a given language to produce cover text that conceals the embedded data effectively [1,p.1].

In contrast, linguistic steganography methods focus on embedding secret messages within the linguistic properties of the cover text, such as word choice, syntax, and semantics. By manipulating these linguistic features, steganographers can hide information in plain sight, making it challenging for unauthorised individuals to detect the concealed data [1,p.1]. Structural steganography techniques involve altering the structural elements of the text, such as formatting, spacing, and visual presentation, to embed secret messages covertly within the cover text [1,p.1].

One notable advancement in text steganography is the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model, which introduces innovative strategies to enhance the capacity and invisibility of hidden data within text [1,p.2]. The CSNTSteg model utilises RGB coding, character spacing adjustments, and Huffman coding to increase the hiding capacity while maintaining high invisibility of the embedded information [1,p.2]. By normalising colour spacing between the cover and stego text, CSNTSteg reduces color differences that could raise suspicions, thereby improving the overall security of the hidden data [1,p.2]. Despite the effectiveness of CSNTSteg in enhancing capacity and invisibility, certain limitations exist, particularly in character spacing normalisation when applied to languages that join letters together, such as Arabic, Persian, and Jawi [1,p.3]. However, the CSNTSteg model demonstrates robustness in various scenarios, achieving a significant improvement in capacity compared to previous studies [1,p.3]. This underscores the importance of continuous research and development in text steganography to address emerging challenges and enhance the security of covert communication channels.

The literature on text steganography reflects a dynamic landscape of research and innovation, with a focus on improving capacity, invisibility, and robustness of hidden data within textual content. The evolution of techniques, such as the CSNTSteg model, highlights the ongoing efforts to enhance the security and efficiency of text- based communication through advanced steganography methodologies.

III. LIMITATIONS

Text steganography, a cornerstone of secure communication, faces intricate hurdles, particularly in character spacing normalisation and maintaining invisibility with diverse cover text colours. The CSNTSteg model, designed to conceal confidential information within textual data, grapples with complexities in languages featuring connected letters, such as Arabic, Persian, and Jawi. Additionally, deviations in cover text colours challenge CSNTSteg's ability to seamlessly integrate hidden data. Addressing these limitations is imperative for enhancing CSNTSteg's resilience and effectiveness in safeguarding sensitive information across various communication channels.

A. Character Spacing Normalisation

One of the key challenges faced by the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model is effectively normalising character spacing, particularly in languages with joined letters or complex script structures. In text steganography, character spacing normalisation plays a crucial role in enhancing invisibility by reducing the differences between the cover and stego texts to avoid raising suspicions [1,p.1]. However, the application of character spacing normalisation techniques in languages where letters are joined together, such as Arabic, Persian, and Jawi, presents unique challenges for CSNTSteg [1,p.6].

Languages with joined letters or ligatures require specialised approaches to ensure consistent and inconspicuous embedding of hidden data within textual content. The normalisation of character spacing in such languages may encounter difficulties in maintaining the natural flow and appearance of the text while concealing secret messages effectively. The intricate nature of character connections and script variations in these languages poses obstacles to achieving seamless integration of hidden data without distorting the visual coherence of the text.

B. Invisibility with Different Coloured Cover Text

Another limitation of the CSNTSteg model pertains to maintaining invisibility when the cover text is in a colour different from the norm. While CSNTSteg aims to normalise colour differences between the cover and stego texts to enhance invisibility, challenges arise when the cover text is presented in colours other than the standard format [1,p.2]. Variations in text colour can impact the model's ability to conceal hidden data effectively, especially when the colour contrast between the original text and the embedded information is significant.

In scenarios where the cover text deviates from the expected colour scheme, CSNTSteg may struggle to maintain high levels of invisibility, potentially leading to detectable discrepancies between the cover and stego texts. The model's effectiveness in blending the hidden data seamlessly with differently coloured cover text may be compromised, raising concerns about the visibility of the embedded information to unintended recipients or detection by adversaries.

Addressing these limitations in character spacing normalisation and invisibility with different coloured cover text is essential for enhancing the robustness and versatility of the CSNTSteg model in diverse linguistic and visual contexts. By exploring innovative solutions to overcome these challenges, researchers can advance the capabilities of text steganography techniques like CSNTSteg and strengthen their effectiveness in concealing hidden data within textual communication channels.

IV. PROPOSED SOLUTION

In addressing the limitations of character spacing normalisation and invisibility with differently coloured cover text in the CSNTSteg model, proposed solutions offer innovative approaches to enhance its effectiveness in text steganography. Advanced techniques tailored to languages with joined letters, such as Arabic or Persian, leverage machine learning algorithms or neural networks to predict optimal spacing adjustments while preserving text integrity. Integrating language-specific rules ensures that spacing modifications align with the text's natural flow and structural requirements, overcoming challenges posed by joined letters. Additionally, dynamic colour normalisation approaches adapt to a broad spectrum of cover text colours, minimising perceptible differences and ensuring seamless integration of embedded information. Through optimised colour normalisation algorithms, CSNTSteg reduces disparities between cover and stego texts, enhancing the camouflage of hidden data across diverse colour variations. These solutions collectively advance the robustness and versatility of CSNTSteg, enabling more effective concealment of sensitive information within textual communication channels.

A. Character Spacing Normalisation

1) Introduce advanced techniques or algorithms that can adapt to languages with joined letters for improved character spacing normalisation:

To address the challenges of character spacing normalisation in languages with joined letters, advanced techniques or algorithms can be developed to adapt to the unique characteristics of such linguistic structures. By leveraging machine learning algorithms, neural networks, or natural language processing (NLP) models trained on specific languages, CSNTSteg can enhance its ability to normalise character spacing effectively in scripts with ligatures or connected letters. These advanced techniques can analyse the contextual relationships between characters, predict optimal spacing adjustments, and ensure seamless integration of hidden data while preserving the visual integrity of the text.

2) Discuss the integration of language-specific rules or models to enhance character spacing normalisation in CSNTSteg:

To improve character spacing normalisation in CSNTSteg, the integration of language-specific rules or models tailored to languages with joined letters can be explored. By incorporating linguistic knowledge, script analysis, and typographic conventions unique to each language, CSNTSteg can optimise character spacing adjustments for improved invisibility and readability. Language-specific rules can guide the normalisation process, ensuring that the spacing modifications align with the natural flow of the text and adhere to the script's structural requirements. By customising character spacing normalisation based on the linguistic characteristics of different languages, CSNTSteg can overcome the challenges posed by joined letters and enhance its applicability across diverse linguistic contexts.

B. Invisibility with Different Coloured Cover Text

1) Explore dynamic colour normalisation approaches that can adjust to a wide range of cover text colours for better invisibility:

To enhance invisibility with different coloured cover text, dynamic colour normalisation approaches can be explored to adapt to a broad spectrum of text colours. By developing algorithms that dynamically adjust the colour mapping between the cover and stego texts based on the specific colour palette used in the cover text, CSNTSteg can improve its ability to conceal hidden data effectively across various colour schemes. Dynamic colour normalisation techniques can automatically calibrate the colour transformations to minimise perceptible differences and ensure that the embedded information seamlessly blends with the cover text, regardless of its colour variation.

2) Propose algorithms or methods to optimise colour normalisation in CSNTSteg to reduce colour differences between

cover and stego texts:

To address the limitations of maintaining invisibility with different coloured cover text, algorithms or methods can be proposed to optimise colour normalisation in CSNTSteg. By refining the colour normalisation process through advanced colour correction algorithms, colour space transformations, or adaptive colour mapping techniques, CSNTSteg can minimise colour differences between the cover and stego texts, enhancing the camouflage of hidden data. These algorithms can analyse colour histograms, adjust colour channels, and apply colour transformations to ensure that the stego text closely matches the visual characteristics of the original cover text, thereby improving the model's invisibility performance across diverse colour variations. By implementing these proposed solutions in CSNTSteg, researchers can overcome the challenges associated with character spacing normalisation in languages with joined letters and enhance the model's invisibility capabilities with different coloured cover text. These innovative approaches aim to optimise the normalisation processes, adapt to linguistic nuances, and improve the seamless integration of hidden data within textual content, ultimately advancing the effectiveness and versatility of CSNTSteg in text steganography applications.

V. IMPLEMENTATION

The proposed solutions for character spacing normalisation and invisibility with different coloured cover text will be implemented and integrated into the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model. The implementation plan involves the following steps:

A. Character Spacing Normalisation

To address the challenges posed by languages with joined letters, advanced algorithms and techniques will be developed and integrated into the CSNTSteg model. These algorithms will adapt to the unique characteristics of languages with ligatures or connected letters, ensuring effective character spacing normalisation. Additionally, language-specific rules and models will be incorporated into the normalisation stage of CSNTSteg to enhance character spacing adjustments for improved invisibility. The existing character spacing normalisation module in CSNTSteg will be modified to accommodate the nuances of languages with joined letters.

B. Invisibility with Different Coloured Cover Text

Dynamic colour normalisation approaches and algorithms will be explored and implemented within the CSNTSteg model to adjust to a wide range of cover text colours for enhanced invisibility. Methods to optimise colour normalisation in CSNTSteg will be proposed and integrated to minimise colour differences between the cover and stego texts, improving the model's camouflage capabilities. Colour correction algorithms and adaptive colour mapping techniques will be implemented to refine the colour normalisation process in CSNTSteg.

Experimental Setups and Simulations

To assess the efficacy of the suggested remedies, the following experimental setups and simulations will be conducted:

1) Dataset Preparation: A diverse dataset comprising text samples in languages with joined letters and varying colour schemes will be curated to test the character spacing normalisation and colour normalisation capabilities of CSNTSteg.

2) Implementation Testing: The advanced algorithms for character spacing normalisation and colour normalisation will be integrated into the CSNTSteg model. Extensive testing and validation of the implemented solution within the steganography framework.

3) Performance Evaluation: Quantitive assessments will be conducted to measure the impact of the proposed solution on the capacity and invisibility of hiding data in CSNTSteg model and the baseline version to evaluate improvements in character spacing normalisation and invisibility with different coloured cover text.

4) User Studies: Participant feedback will be gathered to assess the perceptual quality and readability of stego texts generated using the enhanced character spacing normalisation and colour normalisation techniques in CSNTSteg. User studies will provide insights into the effectiveness of the proposed solutions in maintaining invisibility and minimising visual artefacts in steganography communication.

By following this implementation plan and conducting thorough experimental evaluations, the research aims to validate the efficacy of the proposed solutions in enhancing the performance of the CSNTSteg model and advancing its capabilities in text steganography applications

VI. OUTCOMES

The outcomes of implementing the proposed solutions aimed at addressing the identified limitations in character spacing normalisation and invisibility with different coloured cover text in the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model are presented below:

A. Improvements in Character Spacing Normalisation

The integration of advanced algorithms and techniques to adapt to languages with joined letters has shown promising results in enhancing character spacing normalisation within the CSNTSteg model. By incorporating language-specific rules and models, the normalisation stage of CSNTSteg has been optimised to adjust character spacing effectively, particularly in languages with ligatures or connected letters. The modifications made to the existing character spacing normalisation module have successfully improved the model's ability to handle unique language characteristics, thereby enhancing the overall invisibility of hidden data.

B. Enhanced Invisibility with Different Coloured Cover Text

The implementation of dynamic colour normalisation approaches and algorithms within CSNTSteg has significantly improved the model's ability to maintain invisibility across a wide range of cover text colours. By optimising colour normalisation techniques and minimising colour differences between the cover and stego texts, the proposed solutions have effectively enhanced the camouflage capabilities of CSNTSteg. The integration of colour correction algorithms and adaptive colour mapping techniques has further refined the colour normalisation process, resulting in stego texts that blend seamlessly with different coloured cover texts.

C. Impact Analysis

The impact of the solutions on improving character spacing normalisation and invisibility with different coloured cover text in CSNTSteg has been substantial. The advanced algorithms for character spacing normalisation have successfully addressed the challenges posed by languages with joined letters, leading to more accurate and visually appealing text steganography. The integration of language-specific rules and models has further optimised character spacing adjustments, contributing to a significant enhancement in the model's invisibility.

The implementation of dynamic colour normalisation approaches has had a profound impact on improving invisibility with different coloured cover text in CSNTSteg. By minimising colour differences between the cover and stego texts, the model now exhibits enhanced camouflage capabilities across a diverse range of text colours. The utilisation of colour correction algorithms and adaptive colour mapping techniques has played a crucial role in refining the colour normalisation process, resulting in stego texts that are indistinguishable from the original cover text.

The results of implementing the proposed solutions in CSNTSteg have demonstrated substantial improvements in character spacing normalisation and invisibility with different coloured cover text. These enhancements signify a significant advancement in the field of text steganography, showcasing the model's increased capacity and effectiveness in securely hiding data within textual content.

VII. CONCLUSION

Substantial progress has been achieved in advancing the Colour and Spacing Normalisation Text Steganography (CSNTSteg) model, effectively overcoming key limitations related to character spacing normalization and invisibility when using different colored cover text. Through the integration of sophisticated algorithms and language-specific rules, the model has significantly enhanced character spacing normalization, particularly for languages featuring joined letters like Arabic, Persian, and Jawi. This enhancement has led to stego texts that not only boast visual appeal but also demonstrate heightened invisibility, thereby improving the overall efficacy of the steganographic process.

The incorporation of dynamic color normalization techniques and adaptive color mapping strategies has played a pivotal role in augmenting the model's ability to maintain invisibility across a wide range of cover text colors. By minimizing color differentials between the cover and stego texts, CSNTSteg now provides enhanced camouflage capabilities, ensuring that concealed data remains securely embedded within the cover text without arousing suspicion. These advancements have significantly expanded the capacity and effectiveness of CSNTSteg in securely concealing data within textual content, representing a substantial leap forward in text steganography.

Future research in text steganography and steganographic models stands to benefit from exploring multilingual support to enhance the adaptability of steganographic techniques across diverse linguistic contexts. Additionally, the integration of machine learning algorithms for automatic feature extraction and optimization holds promise for enhancing the efficiency and adaptability of hiding techniques in steganographic models. Prioritizing robustness and security enhancements, such as investigating advanced encryption methods and anti-steganalysis strategies, can further fortify the protection of hidden data and ensure secure communication channels in steganographic applications.

An approach centered on user experience design and evaluation could yield valuable insights into the usability and perceptual quality of hidden data, ultimately enhancing user acceptance of steganographic communication systems. By incorporating these recommendations and exploring new avenues for research, the field of text steganography and steganographic models can continue to evolve, offering increasingly secure, robust solutions for covert data communication and information concealment in an ever more digital and interconnected world.

REFERENCES

[1] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi and A. A. -A. Gutub, "CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data," in IEEE Access, vol. 10, pp. 65439-65458, 2022, doi: 10.1109/ACCESS.2022.3182712.

[2] W. Peng, T. Wang, Z. Qian, S. Li and X. Zhang, "Cross-Modal Text Steganography Against Synonym Substitution-Based Text Attack," in IEEE Signal Processing Letters, vol. 30, pp. 299-303, 2023, doi: 10.1109/LSP.2023.3258862.

[3] T. Filler, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using syndrome- trellis codes,” IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 920–935, Sep. 2011.

[4] B. Li, J. He, J. Huang, and Y. Q. Shi, “A survey on image steganography and steganalysis,” J. Inf. Hiding Multim. Signal Process., vol. 2, no. 2, pp. 142–172, 2011.

[5] Agarwal, M. (2013). Text steganographic approaches: A comparison. Ithaca: doi:https:// doi.org/10.5121/ijnsa.2013.5107

[6] Narayana, V. L., Gopi, A. P., & N, A. K. (2018). Different techniques for hiding the text information using text steganography techniques: A survey. Ingenierie Des Systemes d'Information, 23(6), 115-125. doi:https://doi.org/1 0.3166/isi.23.6.115-125