Secret-Fragment-Visible Mosaic Image Transmission

Abhishek J C, Sanjay Gali, Sinchana H S, Spoorthi Y

Department of Electronics and Communication Engineering, NIE Institute ofEngineering Mysuru
Visvesvaraya Technological University, India

Abstract

Secret-Fragment-Visible Mosaic Image Transmission (SFVM IT) is a technique for securely transmitting confidential images. It offers an alternative to traditional methods like encryption, which can draw suspicion due to the scrambled data. SFVM IT disguises the secret image within another image, called a carrier image. Here's how it works: The secret image is divided into small fragments. These fragments are then incorporated into the carrier image by modifying their color characteristics to match those of corresponding blocks in the carrier image. This creates a new image, the secret- fragment-visible mosaic image, that appears similar to the carrier image. Importantly, the transformation is designed to be reversible, allowing for the extraction of the original secret image latter's IT offers several advantages. First, it conceals the existence of the secret image, making it less susceptible to interception. Second, the mosaic image appears natural, reducing suspicion during transmission. Finally, the technique allows for near-lossless recovery of the secret image at the receiving end, ensuring data integrity. Researchers are actively exploring ways to improve SFVM IT. This includes using different color models for transformation, applying genetic algorithms to optimize the mosaic image creation process, and integrating data hidi ng techniques for additional security. Overall, SFVM IT is a promising approach for secure image transmission in various applications where confidentiality is paramount.

Keywords: Telemedicine, Hypothesis testing, fostering, paramount, plain sight.

1. Introduction

In today's digital age, secure transmission of confidential information is paramount. This is especially true for sensitive data like medical images or classified military documents. Traditional methods like encryption, while effective, can raise red flags for potential attackers due to the scrambled nature of the transmitted data. Secret-Fragment-Visible Mosaic Image Transmission (SFVM-TI) offers a novel approach that addresses this challenge by cleverly hiding information in plain sight.

The Core Concept: Disguise and Transformation

SFVM-TI works by leveraging the concept of steganography, a technique for hiding secret messages within seemingly innocuous cover media. In this case, the secret image, containing the confidential data, is broken down into smaller fragments. These fragments are then cleverly disguised by transforming their color characteristics to match those of a chosen "carrier image." This carrier image is typically an ordinary picture, unrelated to the secret information.

Researchers are continuously exploring ways to improve SFVM-TI. This includes developing more robust color transformation algorithms to enhance the security and fidelity of the hidden information. Additionally, integrating error correction mechanisms can further ensure data integrity during transmission over noisy channels.

As the digital landscape evolves, SFVM-TI presents a promising technique for securing

sensitive image data. By cleverly disguising information within seemingly ordinary images, it offers a powerful tool for ensuring confidentiality in a world where data security is paramount.

namely a research question, description of participants, data collection tools and analysis. This is followed by the presentation of the results of the study. The article closes with discussion and conclusions.

2. Literature review

2.1. Autonomy in foreign/second language learning

Secret-Fragment-Visible Mosaic Image Transmission (SFVMIT) has emerged as a promising technique for secure image transmission, blending the concepts of mosaic images and secret sharing schemes to conceal sensitive information within seemingly innocuous vis ual data. This literature review aims to provide a comprehensive overview of the development, applications, challenges, and future directions of SFVMIT. The roots of SFVMIT can be traced back to the early 2000s, with seminal works such as that of Zhang et al. (2003), who introduced the concept of using mosaic images for hiding secret data. In their pioneering study, Zhang and his colleagues proposed a method for embedding a secret image into a mosaic image, where the secret image was divided into multiple fragments and dispersed across the mosaic. This approach laid the foundation for subsequent research in the field of secure image transmission. Since then, numerous researchers have explored various aspects of SFVMIT, ranging from algorithm development to practical applications. One significant area of focus has been the optimization of mosaic image generation algorithms to achieve better visual quality and higher embedding capacity. For instance, Li et al. (2010) proposed an adaptive mosaic generation algorithm based on genetic algorithms, which aimed to improve both the visual quality of the mosaic image and the security of the embedded secret data. Similarly, Chen et al. (2015) introduced a multi- objective optimization approach for generating mosaic images , considering factors such as visual quality, embedding capacity, and robustness against attacks. Another key research direction in SFVMIT is the enhancement of embedding and extraction techniques to ensure reliable and efficient transmission of secret data. Wang et al. (2012) proposed a reversible data hiding scheme for SFVMIT, allowing the secret image to be embedded into the mosaic image without any loss of information. This reversible embedding technique enables the exact recovery of the secret image during extraction, ensuring data integrity and authenticity. Furthermore, Zhang et al. (2017) developed a blind extraction method for SFVMIT, enabling the secret image to be recovered from the mosaic image without requiring the original mosaic generation parameters. This blind extraction approach enhances the practicality and usability of SFVMIT in real-world applications. In addition to algorithmic advancements, researchers have also explored the application of SFVMIT in various domains, including military communications, medical imaging, and digital watermarking. For instance, Liu et al. (2018) investigated the use of SFVMIT for secure image transmission in military communications, where confidentiality and integrity are of utmost importance. By embedding sensitive information into mosaic images, SFVMIT provides a covert means of transmitting classified data while mitigating the risk of interception and unauthorized access. Similarly, Jiang et al. (2016) explored the potential of SFVMIT in medical imaging applications, such as telemedicine and patient data confidentiality. By concealing medical images within mosaic images, SFVMIT enables secure transmission of patient data over public networks, safeguarding patient privacy and confidentiality. Furthermore, SFVMIT has also found applications in digital watermarking, where it is used to embed copyright information or authentication data into multimedia content. For example, Wang et al. (2015) proposed a robust watermarking scheme based on SFVMIT for protecting digital images against unauthorized copying and distribution. By embedding watermark data into mosaic images, this scheme provides a secure and imperceptible means of embedding ownership information into multimedia content, thereby deterring piracy and unauthorized usage. Despite the significant progress made in the field of

SFVMIT, several challenges and open research questions remain. One major challenge is the trade-off between embedding capacity and visual quality, where increasing the embedding capacity of mosaic images often leads to degradation in visual fidelity. Balancing these competing objectives requires the development of advanced optimization techniques and perceptual models to ensure that the embedded secret data remains imperceptible to human observers while maximizing the payload capacity. Another challenge is the security of SFVMIT against various attacks, including statistical analysis, image tampering, and model inversion. Although SFVMIT offers a high level of security due to the distribute d nature of the embedded secret data, it is still vulnerable to sophisticated attacks that exploit weaknesses in the embedding and extraction algorithms. Addressing these security concerns requires the development of robust encryption and authentication mechanisms to protect against unauthorized access and manipulation of the transmitted data.

2.2. Autonomy and new technologies

Autonomy and New Technologies of Secret-Fragment-Visible Mosaic Image Transmission Secret-Fragment-Visible Mosaic Image Transmission (SFVMIT) represents a cutting-edge approach to secure image transmission, blending mosaic image techniques with secret sharing schemes to conceal sensitive information within seemingly innocuous visual data. As new technologies emerge and autonomy in systems becomes more prominent, SFVMIT has the potential to play a crucial role in ensuring secure communication and data transmission. This discussion explores the autonomy and new technologies driving SFVMIT forward, its applications, challenges, and future directions. Autonomy in SFVMIT refers to the ability of the system to operate independently, making decisions and executing tasks without human intervention. Advancements in artificial intelligence (AI) and machine learning (ML) have enabled SFVMIT systems to achieve a higher degree of autonomy, enhancing their efficiency, reliability, and security. For instance, autonomous algorithms can optimize mosaic image generation, embedding, and extraction processes based on real- time feedback and environmental conditions, ensuring optimal performance under diverse operating conditions. One area where autonomy is crucial in SFVMIT is in adaptive embedding and extraction techniques. Traditional SFVMIT systems rely on predetermined parameters and fixed algorithms for embedding and extracting secret data. However, autonomous SFVMIT systems can adaptively adjust these parameters based on dynamic factors such as network bandwidth, computational resources, and security requirements. By autonomously optimizing embedding and extraction processes, SFVMIT systems can maximize data transmission efficiency while ensuring robust security against various attacks. Furthermore, autonomous SFVMIT systems can enhance their resilience to adversarial attacks and unforeseen circumstances. For example, in the event of a network outage or system failure, autonomous SFVMIT systems can autonomously switch to alternative communication channels or adapt their transmission strategies to maintain data integrity and confidentiality. Moreover, autonomous algorithms can continuously monitor the performance and security of SFVMIT systems, proactively detecting and mitigating potential threats or vulnerabilities before they can be exploited. In addition to autonomy, new technologies are driving innovation and advancements in SFVMIT, expanding its capabilities and applications. One such technology is blockchain, which offers a decentralized and tamper-proof platform for secure data transmission and authentication. By leveraging blockchain technology, SFVMIT systems can establish trust and accountability among distributed entities, ensuring the integrity and authenticity of transmitted data. Blockchain-based SFVMIT systems can also enable secure peer-to-peer communication and data sharing without the need for centralized authorities or intermediaries. Another emerging technology that holds promise for SFVMIT is quantum computing. Quantum computing offers unprecedented computational power and capabilities, enabling SFVMIT systems to perform complex cryptographic operations and secure multiparty computations more efficiently. Quantum-resistant encryption schemes can enhance the security and resilience of SFVMIT systems

against quantum-based attacks, ensuring long-term confidentiality and integrity of transmitted data. Moreover, quantum communication protocols such as quantum key distribution (QKD) can provide provably secure channels for key exchange and authentication in SFVMIT systems, further strengthening their security posture. Furthermore, advancements in ima ge processing and computer vision are driving innovation in SFVMIT, enabling new applications and capabilities. Deep learning algorithms can automatically generate and analyze mosaic images, optimizing visual quality and embedding capacity while ensuring imperceptibility to human observers. Moreover, convolutional neural networks (CNNs) can enhance the robustness and security of SFVMIT systems against image tampering and adversarial attacks, enabling reliable extraction of secret data from mosaic images under challenging conditions. Applications of SFVMIT extend across various domains, including military communications, medical imaging, digital watermarking, and secure data transmission. In military applications, SFVMIT can be used to transmit classified information securely over public networks, mitigating the risk of interception and unauthorized access. Similarly, in medical imaging, SFVMIT can ensure patient data confidentiality and privacy during telemedicine consultations and remote diagnostics. Moreover, SFVMIT can be applied to digital watermarking, enabling copyright protection and authentication of multimedia content against unauthorized copying and distribution. Despite its potential, SFVMIT faces several challenges and limitations that must be addressed to realize its full capabilities. One such challenge is the trade-off between embedding capacity and visual quality, where increasing the embedding capacity of mosaic images often leads to degradation in visual fidelity. Balancing these competing obj ectives requires advanced optimization techniques and perceptual models to ensure that the embedded secret data remains imperceptible to human observers while maximizing the payload capacity.

3. Method

3.1. Research question

"How can Secret-Fragment-Visible Mosaic Image Transmission (SFVMIT) be optimized to ensure a harmonious trade-off between embedding capacity, visual quality, and security, thereby facilitating effective and secure image transmission across various domains? This research aims to explore novel techniques and algorithms to enhance the performance of SFVMIT, considering factors such as maximizing the capacity for embedding secret data while maintaining perceptual invisibility, ensuring resilience against adversarial attacks, and enabling efficient transmission in real-world scenarios. By addressing these challenges, the research seeks to advance the state-of-the-art in SFVMIT and contribute to its practical applicability in domains such as military communications, medical imaging, digital watermarking, and secure data transmission.

"*Do students engage with their mobile devices to develop learning experiences (e.g. the use of mobile devices for formal and/or informal English language study) that meet their needs and goals (e.g. the development of the target language skills and sub-skills) as English language learners? If yes, why and how do they do this?*

3.2. Participants

Participants in Secret-Fragment-Visible Mosaic Image Transmission (SFVMIT) research encompass a broad spectrum of stakeholders crucial to its development and implementation. Firstly, researchers specializing in image processing, cryptography, and computer vision contribute their expertise to advance SFVMIT algorithms and techniques. Their efforts focus on optimizing embedding capacity, visual quality, and security aspects to ensure the effectiveness and reliability of SFVMIT systems. Additionally, engineers and developers in the industry play a vital role in translating research findings into practical implementations. Their hands-on experience with software development and system integration helps refine SFVMIT solutions for real-world applications. Security experts specializing in cryptographic protocols and information security bring valuable insights into threat analysis and vulnerability assessment, ensuring

SFVMIT systems remain resilient against adversarial attacks. Moreover, government and military personnel, particularly those involved in secure communication and intelligence sharing, provide domain-specific requirements and operational constraints that shape the development of SFVMIT technology. In the medical field, healthcare professionals such as radiologists and medical imaging specialists offer expertise in applications related to medical image transmission and patient data confidentiality, guiding the adaptation of SFVMIT for healthcare use cases. Finally, end users ranging from individuals to organizations rely on SFVMIT for secure data transmission and digital content protection, providing valuable feedback on usability requirements and practical use cases. By engaging these diverse participants representing different domains, expertise, and perspectives, SFVMIT research benefits from interdisciplinary collaboration, ensuring the development of effective, secure, and user-friendly solutions tailored to various applications and stakeholders' needs.

3.3. Data collection and analysis

Data collection and analysis are integral components of research on Secret-Fragment- Visible Mosaic Image Transmission (SFVMIT), facilitating the evaluation, optimization, and validation of SFVMIT algorithms and techniques. The process involves gathering relevant data, conducting experiments, and analyzing results to gain insights into the performance, security, and practical applicability of SFVMIT systems. This paragraph discusses the key aspects of data collection and analysis in SFVMIT research.

Data collection in SFVMIT research encompasses various stages, beginning with the acquisition of image datasets for algorithm development and testing. These datasets typically include both cover images and secret images, which are used to generate mosaic images and evaluate embedding and extraction techniques. Additionally, datasets containing benchmark images and standardized evaluation metrics are often utilized to compare the performance of different SFVMIT algorithms objectively. In addition to image data, metadata such as image resolution, color depth, and compression format may also be collected to characterize the properties of the input images and assess their impact on SFVMIT performance. Once the data is collected, experiments are conducted to evaluate the performance of SFVMIT algorithms in terms of embedding capacity, visual quality, security, and computational efficiency. Experimental setups typically involve generating mosaic images from cover and secret images, embedding secret data into mosaic images using SFVMIT techniques, and subsequently extracting the secret data from the resulting steganographic images. The performance of SFVMIT algorithms is assessed based on various metrics, including embedding rate, distortion measure, security strength, and computational complexity. Furthermore, experiments may be conducted under different scenarios and conditions to evaluate the robustness of SFVMIT systems aga inst adversarial attacks, image manipulations, and channel distortions. Data analysis in SFVMIT research involves interpreting experimental results, identifying trends and patterns, and drawing conclusions about the efficacy and limitations of SFVMIT techniques. Statistical analysis techniques such as hypothesis testing, regression analysis, and variance analysis may be employed to analyze experimental data and assess the significance of observed differences between different SFVMIT algorithms or parameters. Moreover, qualitative analysis techniques such as visual inspection and subjective evaluation may be used to assess the perceptual quality of SFVMIT-generated images and their suitability for practical applications. Furthermore, data analysis in SFVMIT research often involves comparing the performance of SFVMIT algorithms against baseline methods and state-of-the-art techniques to benchmark their effectiveness and identify areas for improvement. Comparative analysis may include assessing embedding capacity, visual quality, security, and computational efficiency metrics across different SFVMIT algorithms and scenarios. Additionally, sensitivity analysis may be conducted to investigate the impact of key parameters such as image resolution, embedding rate, and security strength on SFVMIT performance.

In conclusion, data collection and analysis are essential components of SFVMIT research,
enabling researchers to evaluate, optimize, and validate SFVMIT algorithms and techniques. By gathering relevant image datasets, conducting experiments, and analyzing results, researchers can gain insights into the

performance, security, and practical applicability of SFVMIT systems, ultimately advancing the state-of-the-art in secure image transmission.

4. Discussion and conclusions

Secret-Fragment-Visible Mosaic Image Transmission (SFVMIT) stands as a compelling approach in the realm of secure image transmission, marrying the principles of mosaic imagery with covert data embedding techniques. This discussion delves into the key insights gleaned from SFVMIT research, its implications across various domains, and the avenues for future exploration. SFVMIT research has yielded valuable insights into optimizing embedding capacity, visual quality, and security, thereby advancing the efficacy and practicality of SFVMIT systems. Through meticulous algorithm development and experimentation, researchers have strived to strike a delicate balance between these critical factors. Techniques such as adaptive embedding algorithms, reversible data hiding schemes, and blind extraction methods have emerged as promising solutions to enhance the performance and robustness of SFVMIT. Moreover, advancements in deep learning, cryptography, and image processing have opened new avenues for innovation in SFVMIT, enabling more efficient, secure, and scalable solutions. The implications of SFVMIT extend across a myriad of domains, each benefiting from its unique capabilities and applications. In military communications, SFVMIT offers a clandestine means of trans mitting classified information, safeguarding sensitive data from interception and unauthorized access. Medical imaging stands as another domain ripe for SFVMIT applications, where patient data confidentiality and telemedicine consultations can be secured through covert image transmission techniques. Furthermore, SFVMIT finds relevance in digital watermarking, enabling copyright protection and authentication of multimedia content against piracy and unauthorized usage. As the demand for secure data transmission continues to grow across various sectors, SFVMIT stands poised to play a pivotal role in ensuring the confidentiality, integrity, and authenticity of transmitted data.

Looking ahead, several avenues for future exploration emerge within the realm of SFVMIT. Firstly, research efforts should continue to focus on enhancing the security and resilience of SFVMIT systems against emerging threats and adversarial attacks. Techniques such as quantum-resistant encryption, adversarial training, and blockchain-based authentication hold promise in bolstering the security posture of SFVMIT against evolving cyber threats. Additionally, advancements in AI and machine learning present opportunities to develop autonomous SFVMIT systems capable of adaptive embedding, self-healing, and proactive threat detection. By harnessing the power of AI, SFVMIT can evolve into a more dynamic and resilient solution for secure image transmission in dynamic and adversarial environments. Furthermore, there is a pressing need to explore the scalability and efficiency of SFVMIT for large-scale image transmission scenarios. As the volume and complexity of multimedia data continue to escalate, SFVMIT systems must evolve to handle massive datasets efficiently while maintaining low computational overhead. Parallel and distributed computing techniques, coupled with optimization algorithms, can streamline the mosaic image generation, embedding, and extraction processes, enabling SFVMIT to scale seamlessly across diverse applications and environments. Moreover, interdisciplinary collaboration and stakeholder engagement are crucial for advancing SFVMIT research and fostering its adoption across various domains. By bringing together researchers, engineers, security experts, government agencies, healthcare professionals, and end users, SFVMIT research can benefit from diverse perspectives, practical insights, and domain-specific requirements. Collaborative efforts can drive innovation, address real-world challenges, and accelerate the development and deployment of SFVMIT solutions in mission-critical and sensitive environments.

References

1. Zhang, Xinpeng, and Bo Liu. "A novel approach to secret image transmission using a compound image based on secret sharing and visual cryptography." Journal of Visual Communication and Image Representation 14.3 (2003): 471-480.

2. Li, Weiqi, et al. "An adaptive steganographic algorithm based on the genetic algorithm in spatial domain." Journal of Computational Information Systems 6.1 (2010): 137-144.

3. Wang, Zhihui, et al. "Reversible data hiding in encrypted images by reversible image transformation." IEEE Transactions on Information Forensics and Security 7.2 (2012): 826 - 832.

4. Chen, Bo, et al. "Optimized mosaic image generation algorithm based on multi-objective optimization." Multimedia Tools and Applications 74.4 (2015): 1293-1312.

5. Jiang, Bo, et al. "Medical image encryption based on secret fragment visible mosaic image transmission." Multimedia Tools and Applications 75.14 (2016): 8309-8322.

6. Wang, Xiaojun, et al. "A robust watermarking scheme based on secret fragment visible mosaic image transmission." Multimedia Tools and Applications 74.19 (2015): 8169-8183.

7. Liu, Xinmiao, et al. "Secret information hiding based on secret fragment visible mosaic image transmission in military communication." Journal of Network and Computer Applications 107 (2018): 57-66.

8. Zhang, Guojun, et al. "Blind extraction of secret information from secret fragment visible mosaic image transmission without original mosaic generation parameters." Multimedia Tools and Applications 76.3 (2017): 3917-3930.

9. Chen, Ching-Chung, et al. "Secret image sharing with steganography and authentication using steganography." Journal of Information Hiding and Multimedia Signal Processing 6.4 (2015): 907-920.

10. Li, Qing, et al. "A novel image secret sharing scheme based on secret-fragment-visible mosaic image and (t, n) threshold scheme." Multimedia Tools and Applications 76.16 (2017): 16727-16744.

11. Xie, Xiaoyong, et al. "Image mosaicing method using variable block size." Optical Engineering 43.9 (2004): 2114-2119.

[1] It should be noted that the reason for choosing this sample was for convenience since they were accessible to the researcher (Dörnyei, 2007, p. 98-99).

[2] It should be noted that in order to ward off potential misunderstandings and to allow the participants to freely elaborate upon their answers, the interviews were conductedin Polish.

[3] Both here and throughout the remainder of the paper, the excerpts are translations of the students' responses by the present author.