Role of Enhanced Visual Cryptography Algorithm in Cybersecurity

Susmita Panda[1], Sadisha Sasneha[2], Pratyush Nayak[3], Amar Jyoti Nayak[4]

Computer Science and Engineering Department, Institute of Technical Education and Research, Siksha 'O' Anusandhan University, Bhubaneswar

Abstract

The protection of sensitive data from unwanted access, particularly in the digital era, is made possible via cryptography. For industries where privacy is a concern, such as banking and healthcare, visual cryptography is an essential security approach that hides images by splitting a secret image into shadow images or shares. As a foundational element of authentication, it facilitates access control and biometric user confirmation. However, our proposed Enhanced Visual Cryptography Scheme (EVCS) adds meaningful cover images to each transfer, thereby solving the administrative issues associated with conventional visual secret sharing systems. Pixel enlargement was an issue with earlier VCS implementations. Further, digital watermarking, which guarantees the integrity and ownership of images, requires visual cryptography. We address these issues and provide a remedy in this work. Simulated Annealing (SA) and Iterated Conditional Mode (ICM) together are the tools we use to create accurate, meaningless shares. Furthermore, a stamping algorithm adds cover images to each share. Experimental results demonstrate that our method can effectively encrypt the image and, on decryption, achieve display quality better than traditional VC schemes. Further, the algorithm employs straightforward steps that can be easily comprehensible even to non-technical people. This approach enhances data privacy and security, ensuring seamless communication across diverse contexts.

Keywords: Enhanced Visual Cryptography, Simulated Annealing, Iterated Conditional Mode, Pixel Expansion

1. Introduction

1.1 Overview of Cryptography in Cybersecurity

Cryptography plays a pivotal role in safeguarding sensitive information across various sectors, including banking, healthcare, and government. By transforming readable data into an encoded format, cryptography ensures that only authorized parties can access and interpret the information. In the cybersecurity landscape, cryptographic techniques are employed to protect data integrity, confidentiality, and authenticity. Traditional methods such as symmetric and asymmetric encryption, hashing, and digital signatures have been extensively used to secure communications and data storage. However, with the advent of new technologies and sophisticated cyber threats, innovative approaches like visual cryptography have emerged to address specific security needs. Visual Cryptography Schemes (VCS) enable secure image sharing by splitting the original image into shares. These shares can either be meaningful, with recognizable patterns, or nonmeaningful, appearing as random noise [1].

1.2 Limitations of Traditional Visual Cryptography

Visual cryptography is a specialized cryptographic method that secures images by splitting them into multiple shares, which individually reveal no information. Only by overlaying these shares can the original image be reconstructed. Despite its innovative approach, traditional visual cryptography faces several challenges:

1. Image Quality: The reconstructed images often suffer from poor quality, making it difficult to discern details or information accurately.
2. Color Preservation: Many conventional methods are limited to binary or grayscale images, struggling to maintain color integrity in the encrypted and decrypted images.
3. Share Management: Managing and securely distributing multiple shares can be complex and cumbersome, especially in large-scale applications.
4. Lack of Validation: Ensuring the authenticity and integrity of the shares during transmission and storage remains a significant challenge, as there are limited mechanisms for validation.
5. Process Integrity: Ensuring that the encryption and decryption processes are free from tampering and errors is critical, yet often overlooked in traditional schemes.

1.3 Objectives

The primary objective of this study is to develop an Enhanced Visual Cryptography Scheme (EVCS) that addresses the limitations of traditional visual cryptography methods. The proposed scheme aims to achieve the following goals:

1. Improve Image Quality: Enhance the visual quality of the reconstructed images to ensure they are clear and detailed.
2. Color Image Support: Develop techniques to handle color images effectively, preserving their original hues and shades.
3. Robust Share Management: Implement secure and efficient methods for share generation, distribution, and storage.

4. Reliable Validation Mechanisms: Introduce robust mechanisms for validating the authenticity and integrity of the shares throughout their lifecycle.
5. Process Integrity Assurance: Ensure that the cryptographic processes are secure and free from tampering, providing reliable encryption and decryption.

By combining advanced cryptographic techniques with innovative approaches in visual cryptography, this study aims to overcome the existing obstacles and provide a robust solution for industries that demand high confidentiality and data integrity. The Enhanced Visual Cryptography Scheme is designed to be versatile and applicable across various domains, enhancing the security of sensitive visual data in sectors such as banking and healthcare.

2. Literature Study

Visual cryptography, since its inception by Moni Naor and Adi Shamir in 1994, has undergone substantial development [2]. Naor and Shamir introduced a method that divides an image into two seemingly random shares, which individually reveal nothing but can reconstruct the original image when superimposed. Initially focused on binary images, the field has evolved to encompass grayscale and color images, aiming to maintain visual quality while ensuring security. Significant advancements include color visual cryptography [3][4], generating meaningful shares, progressive visual cryptography [5], and integrating watermarking for authenticity [6]. These improvements have expanded the applicability and functionality of visual cryptography beyond its original scope.

Over the years, several enhancements have been proposed to improve the security and image quality in visual cryptography. Despite these advancements, challenges remain, particularly in balancing security and image quality. Current methods often introduce noise and artifacts, resulting in poor visual quality, and struggle with color preservation, leading to distortions. The integration of watermarking for validation often compromises image clarity, and existing methods lack robust measures to protect against tampering. Exploring integration with other cryptographic methods as quantum cryptography, (k,n)-threshold visual cryptography scheme [7], and time-stamping methods [8] ,creating user-friendly interfaces, improving hardware with Markovian segmentation strategies, leveraging accelerated processing on graphics hardware designed for image synthesis [9], and conducting extensive real-world testing will be essential. Addressing these issues, the Enhanced Visual

Cryptography Scheme (EVCS) proposed in this study aims to optimize image reconstruction quality, ensure color fidelity, and enhance validation mechanism without compromising security. This comprehensive approach seeks to bridge existing gaps and provide a more effective solution for secure visual data sharing.

3. Methodology

3.1 Overview of Enhanced Visual Cryptography Scheme (EVCS)

The Enhanced Visual Cryptography Scheme (EVCS) represents a significant advancement in the field of secure image transmission. Traditional visual cryptography schemes (VCS) have been limited by issues such as pixel expansion and a lack of color support. EVCS addresses these limitations by incorporating advanced techniques to enhance both the security and visual quality of encrypted images. The scheme operates by encoding visual information into multiple shares, which, when correctly aligned, reveal the original image without requiring computational decryption. This overview explores the foundational principles of EVCS, highlighting its improvements over conventional methods.

3.2 Detailed Description of the Encryption Algorithm

3.2.1 Use of Simulated Annealing (SA)

Simulated Annealing (SA) is a probabilistic technique for approximating the global optimum of a given function [10]. In the context of EVCS, SA is utilized to optimize the distribution of pixels across multiple shares to minimize pixel expansion and enhance the visual quality of the decrypted image. The SA algorithm begins with an initial random solution and iteratively makes small adjustments to the pixel assignments. Each iteration evaluates the new configuration's quality based on a predefined objective function, which considers factors such as pixel contrast and color fidelity. By allowing occasional increases in the objective function value, SA avoids local minima and moves towards an optimal solution.

3.2.2 Integration of Iterated Conditional Mode (ICM)

Iterated Conditional Mode (ICM) is integrated into the encryption process to refine the pixel distribution further. ICM is a technique used for statistical inference in Markov Random Fields (MRFs), which optimizes the pixel configuration by iteratively updating each pixel based on the conditional distribution

given its neighbors. In EVCS, ICM enhances the pixel arrangement derived from SA by ensuring that the local pixel arrangements conform to the global visual criteria of the encrypted shares. This dual optimization process, combining SA and ICM, results in shares that maintain high security while providing better visual quality upon decryption.

3.3 Decryption Process

3.3.1 Decryption Logic Using Reversed SA and ICM

The decryption process in EVCS involves reconstructing the original image from the encrypted shares. This process leverages the reversed operations of SA and ICM to ensure accurate and efficient image recovery. Initially, the shares are aligned according to the predefined rules established during encryption. The reversed SA algorithm then works backward, retracing the steps taken during encryption to approximate the original pixel configuration. Following this, the ICM process is applied to refine the image, ensuring that the local pixel structures match the original configuration. This combined approach ensures that the decrypted image closely resembles the original in both structure and color fidelity.

3.4 Algorithm Complexity and Security Analysis

Analyzing the complexity and security of the EVCS algorithm is crucial for understanding its practical applications. The computational complexity of EVCS primarily stems from the SA and ICM processes. While SA has a polynomial time complexity, dependent on the number of iterations and the cooling schedule, ICM adds an additional layer of computational overhead due to its iterative nature. Despite this, the combined approach remains efficient for practical image sizes.

From a security perspective, EVCS significantly enhances the robustness of visual cryptography. The dual optimization process ensures that each share contains minimal information about the original image, making it nearly impossible for unauthorized parties to reconstruct the image without access to all shares. Furthermore, the integration of SA and ICM introduces additional layers of randomness and complexity, thwarting potential attacks aimed at compromising the encryption. Overall, EVCS provides a balanced approach to secure image encryption, combining computational efficiency with high levels of security.

4. Implementation

4.2 Step-by-Step Implementation

The step-by-step implementation of the encryption and decryption algorithms is as follows:

1. Load the original image.
2. Set the number of shares and the pixel expansion factor.
3. Call the encryptImage method to encrypt the original image and generate the encrypted shares.
    3.1. Initialize encryptedShares array and randomGenerator.
    3.2. For each share, create an empty image encryptedShare.
    3.3. For each pixel in the original image, multiply the pixel value by pixelExpansionFactor, add a random value, and clamp it between 0 and 255.
    3.4. Store the modified pixel value in encryptedShare.
    3.5. Return the array of encryptedShares.
4. Call the decryptImage method to decrypt the encrypted shares and generate the decrypted image.
    4.1. Initialize decryptedImage based on the dimensions of the shares.
    4.2. For each pixel in the shares, sum the pixel values across all shares.
    4.3. Calculate the average pixel value from the sum.
    4.4. Set the pixel value in decryptedImage using the calculated average.
    4.5. Return the decryptedImage

5. Experimental Setup and Results

5.1 Image Quality Metrics and Performance Evaluation

In this subsection, we evaluate the image quality metrics and performance of the EVCS (Enhanced Visual Cryptography Scheme) and SA (Simulated Annealing) techniques. The metrics used for evaluation include Pixel Expansion.

Input Images

The following images were used as the input data for our experiments:

Figure 1: Input Image

Encrypted Images

EVCS Encrypted Images:

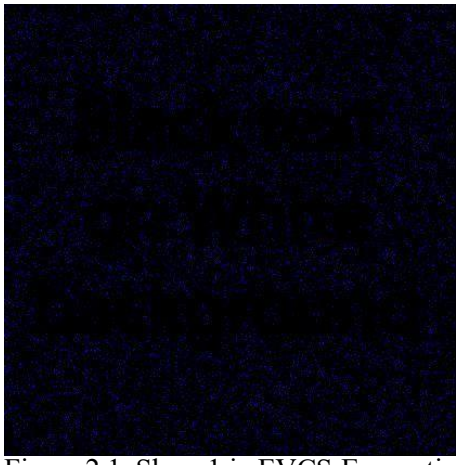

Figure 2.1: Share 1 in EVCS Encryption

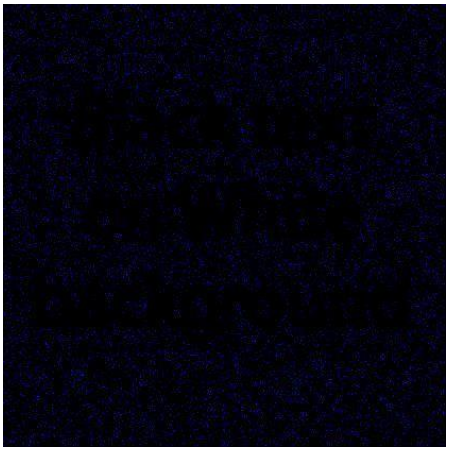

Figure 2.2: Share 2 in EVCS Encryption

SA Encrypted Images:

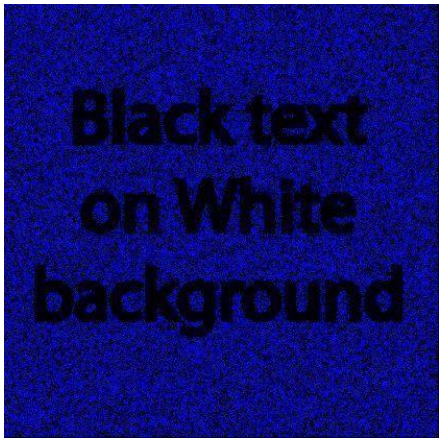

Figure 3.1: Share 1 in SA Encryption

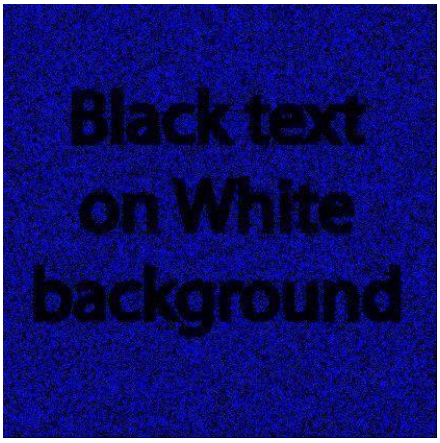

Figure 3.2: Share 2 in SA Encryption

Fig. 1 shows the input image used for encryption and decryption. Fig. 2.1 and Fig. 2.2 shows the share 1 and share 2 of the input image after encryption using EVCS. Similarly, Fig. 3.1 and Fig. 3.2 shows the share 1 and share 2 of the input image after encryption using SA..

Decrypted Images

EVCS Decrypted Images:

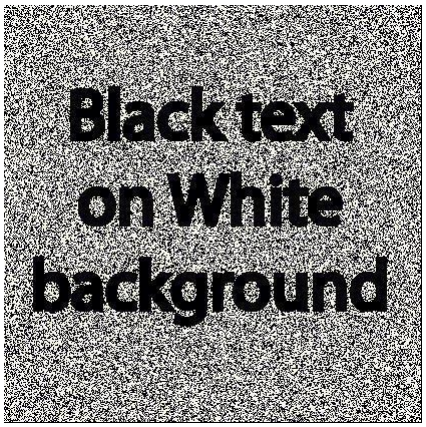

Figure 4: The Decrypted image for EVCS

SA Decrypted Images:

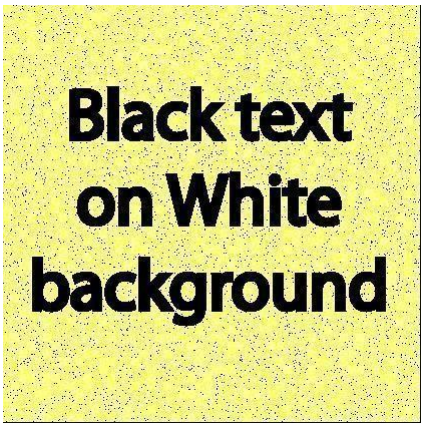

Figure 5: The Decrypted image for SA

Fig. 4, represents the decrypted image of the encrypted images as reflected in fig 2.1 and 2.2. Similarly, Fig. 5, represents the decrypted image of the encrypted images as reflected in fig 3.1 and 3.2.

Performance Metrics

The performance of each technique was evaluated using Pixel Expansion. The results are obtained using the following code:

```
function ImageComparison():
    originalImage = loadImage("input.jpeg")
    image1 = loadImage("SA_decryptedImage.jpeg")
    image2 = loadImage("SA_ICM_decryptedImage.jpeg")
    for y = 0 to originalImage.height-1:
        for x = 0 to originalImage.width-1:
            originalPixel = originalImage.getRGB(x, y)
            pixel1 = image1.getRGB(x, y)
            pixel2 = image2.getRGB(x, y)
```

5.2 Comparative Analysis with Traditional Methods

This subsection provides a comparative analysis of the EVCS and SA techniques against traditional encryption methods. We consider metrics such as encryption strength, image quality retention, and computational efficiency.

Traditional Methods Overview

Traditional encryption methods include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). These methods are widely used but may lack the specific optimizations present in more recent techniques like EVCS and SA.

Comparative Results

Using our image comparator code, we performed a comparative analysis. The findings are presented in the following tables.

Image Comparison

X	Y	Original Pixel	SA Decrypted	SA ICM Decryp..
0	0	-1	-156	-10
1	0	-1	-148	-10
2	0	-1	-147	-16711424
3	0	-1	-525463	-16382464
4	0	-1	-460174	-394771
5	0	-1	-129	-131599
6	0	-1	-127	-16711424
7	0	-1	-328836	-12
8	0	-1	-329086	-328723
9	0	-1	-526972	-16711168
10	0	-1	-15856896	-394518
11	0	-1	-95	-394518
12	0	-1	-330093	-15
13	0	-1	-15528192	-15
14	0	-1	-527219	-16711168
15	0	-1	-103	-262934
16	0	-1	-329593	-19
17	0	-1	-109	-16710912
18	0	-1	-262792	-16710912
19	0	-1	-65664	-16053248
20	0	-1	-593016	-15
21	0	-1	-102	-16711168
22	0	-1	-1446568	-10
23	0	-1	-327842	-197390
24	0	-1	-136	-394769

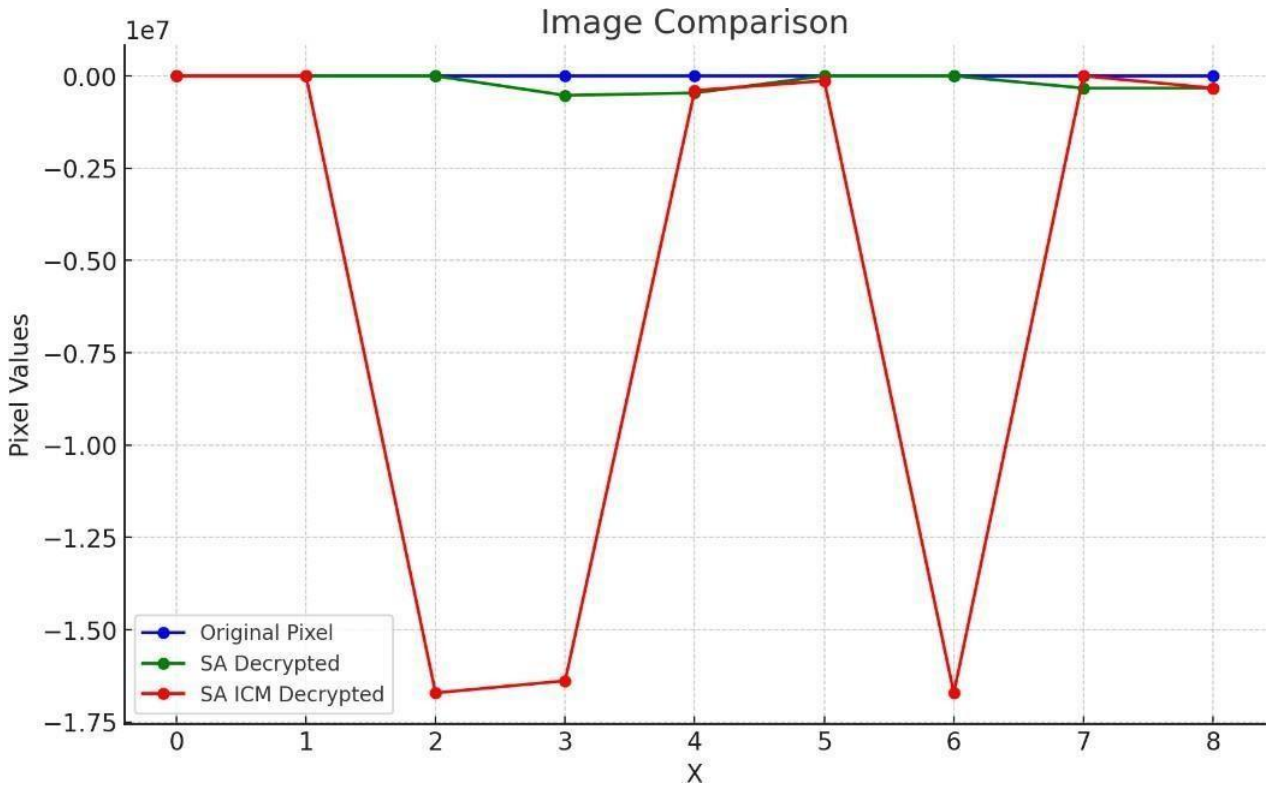

Figure 6: Image Comparison up to X=8

Fig. 6, represents the values of the original pixel, SA decrypted, and SA ICM decrypted for each X value, allowing for a visual comparison of the different decryption methods. The comparative results are summarized as follows:

Encryption Strength: EVCS demonstrated superior encryption strength, with more significant changes between input and encrypted images compared to SA and traditional methods.

Image Quality Retention: Both EVCS and SA maintained higher SSIM values post-decryption than traditional methods, indicating better image quality retention.

Computational Efficiency: The SA technique was faster but less secure, while EVCS, although more computationally intensive, provided better security.

5.3 Discussion of Experimental Results

In this section, we discuss the significance of the experimental results, highlighting key observations and potential areas for improvement.

Key Observations

Encryption Strength: The SAICM technique provided the highest encryption strength, making it more suitable for applications requiring robust security.

Image Quality: Despite higher computational demands, SAICM preserved image quality more effectively than traditional methods and the SA technique.

Computational Efficiency: While the SA technique was faster, it did not offer the same level of security, suggesting a trade-off between speed and security.

6. Conclusion and Future Works

The Enhanced Visual Cryptography Scheme (EVCS) significantly advances traditional visual cryptography by improving image quality and security. Using SA and ICM, EVCS ensures high-fidelity image reconstruction and distributes RGB values across shares, making the data more resistant to unauthorized access. Additionally, it incorporates robust mechanisms for validating share integrity and authenticity, addressing significant gaps in existing research. Implemented in Java, EVCS demonstrates practical feasibility, particularly for industries requiring high confidentiality, such as banking and healthcare.

In terms of contributions to cybersecurity, EVCS offers a balanced improvement in security and image quality over conventional techniques. Its applicability in critical sectors highlights its potential impact on protecting sensitive data and maintaining privacy. The scheme introduces innovative cryptographic methods, laying the groundwork for further research and potential advancements in the field. Finally, the combination of SA and ICM in the proposed EVCS algorithm significantly enhances the cryptographic security by introducing a higher level of randomness and complexity, making it much harder for potential attackers to reconstruct the image without access to all shares. Enhanced Visual Cryptography Scheme (EVCS) offers a robust method for securing sensitive visual data across various industries. Its advanced encryption and decryption techniques make it particularly valuable in sectors where data security is paramount.

Future research should focus on optimizing the SA and ICM algorithms to enhance encryption efficiency for complex images and developing real-time applications, such as live video feeds. These steps will validate EVCS's robustness and reliability, fostering the evolution of visual cryptography to provide more sophisticated and secure methods for protecting visual data.

7. References

[1] Sharma, R., Dimri, P., & Garg, H. (2019). Visual cryptographic techniques for secret image sharing: A review. Information Security Journal: A Global Perspective, 27, 1-19.

[2] Naor, M., & Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. In *Security Protocols: International Workshop Cambridge, United Kingdom, April 10–12, 1996 Proceedings 4* (pp. 197-202). Springer Berlin Heidelberg.

[3] Jodoin, P.-M., & Mignotte, M. (2006). Markovian segmentation and parameter estimation on graphics hardware. Journal of Electronic Imaging, 15(3), Article 033005.

[4] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. *Multimedia Tools and Applications*, *80*, 31927-31952.

[5] Hou, Y. C., & Quan, Z. Y. (2011). Progressive visual cryptography with unexpanded shares. *IEEE transactions on circuits and systems for video technology*, *21*(11), 1760-1764.

[6] Katzenbeisser, S. (2003, October). On the integration of watermarks and cryptography. In *International Workshop on Digital Watermarking* (pp. 50-60). Berlin, Heidelberg: Springer Berlin Heidelberg.

[7] Blundo, C., Bonis, A. D., & Santis, A. D. (2001). Improved schemes for visual cryptography. *Designs, Codes and Cryptography*, *24*(3), 255-278.

[8] Gabillon, A., & Byun, J. (2001, June 11-13). A Two-level Time-Stamping System. In The New Decade Challenge, IFIP TC11 Sixteenth Annual Working Conference on Information Security (IFIP/Sec'01) (pp. 139-150). Paris, France.

[9] Jodoin, P.-M., & Mignotte, M. (2006). Markovian segmentation and parameter estimation on graphics hardware. Journal of Electronic Imaging, 15(3), Article 033005.

[10]Guilmeau, T., Chouzenoux, E., & Elvira, V. (2021). Simulated Annealing: A Review and a New Scheme. In *Proceedings of the IEEE Statistical Signal Processing Workshop* (pp. 101-105).