 ISSN:2302-8149
e-ISSN:2540-9719

An Extended Approach for Color Image Authentication and Recovery Against Composite Attacks

[1]Maher AL Dbsawie*, [2]Suleiman Alassly, [3]Hasan Al Jabbouli
[1]Department of Software Engineering, Informatics Engineering, University of Idlib, Idlib, Syria
[2]Department of Digital communications, Electrical Engineering, University of Idlib, Idlib, Syria
[3]Department of Computer Science, University of New York, New York, USA
*e-mail: maher_adel_al_dbsawie@idlib.edu.sy

(***received*:** 30 July 2026, ***revised*:** 4 August 2026, ***accepted*:** 5 August 2026)

Abstract

This paper proposes an extended approach for color image authentication and recovery utilizing the alpha layer and a secret sharing scheme to counter sequential composite attacks. Building upon our previous work which proved effective against traditional single attacks such as cropping, noise, and superimposition this study addresses the complex challenges posed by successive and combined manipulations. The proposed approach embeds authentication and recovery data within the alpha channel using a spatial correlation phase, ensuring that authentication and repair data are embedded in non-contiguous blocks to guarantee high accuracy in tamper detection and image restoration. Experimental results on diverse color images demonstrate remarkable efficiency in withstanding sequential composite attacks, recording outstanding values of (PSNR = 32.85 dB) and (SSIM = 0.95) even under the most severe composite sequential attacks. This demonstrates exceptional robustness against tampering while preserving the high visual quality of both the stego and recovered images. Ultimately, the findings confirm that this framework significantly enhances the reliability and security of image transmission and storage compared to conventional methodologies.

Keywords: alpha layer, color image authentication, image recovery, secret sharing, sequential composite attacks, tamper detection.

1. Introduction:

In our contemporary digital era, images play a crucial role in storing, preserving, and transmitting sensitive and confidential information. With the growing reliance on digital technologies, the secure transmission of images over the Internet has become an urgent necessity. Digital images are particularly vulnerable because advanced image processing techniques now allow imperceptible modifications to their content, threatening the integrity and authenticity of the stored information [1]. Ensuring the integrity of color images, especially confidential documents, has thus become a critical challenge.

To address these concerns, various authentication and recovery techniques have been proposed [1][2][3]. Among the most effective is our previously developed methodology [4], which relies on secret sharing, dividing sensitive information into multiple shares and ensuring that the original data can only be restored when a predefined number of shares are combined. When integrated with the alpha channel of color images where both embedding quality and embedding efficiency are ensured [5], secret sharing provides a secure and imperceptible means to embed authentication and recovery data without altering the visible content. This combination enables both tamper detection and accurate restoration of compromised images.

Although our previous methodology demonstrated robustness against conventional single attacks such as cropping, text attacks, and noise (Gaussian noise or salt-and-pepper noise) [4]. sequential composite attacks, involving multiple successive manipulations, present a new and complex challenge. Such attacks can significantly compromise image integrity, as multiple attacks are applied

 ISSN:2302-8149
e-ISSN:2540-9719

consecutively, making tampering cumulative. This accumulation renders conventional authentication and recovery algorithms less effective, potentially undermining the overall reliability of the system.
This study aims to extend the scope of our previous methodology by integrating secret sharing with alpha layer embedding to combat sequential composite attacks. This work addresses the limitations of prior studies including our previous work as handling this type of successive and combined attacks remains an unexplored domain in current literature. The proposed framework ensures exceptional robustness against tampering while preserving the visual quality of both the stego images and the recovered images, providing a reliable solution for the secure authentication and restoration of color images in sensitive applications, such as the secure transmission and storage of confidential documents.

2. Literature Review

In this section, some robust methodologies for color image authentication and recovery will be presented. However, these studies based their results on a single, specific attack on color images, which are as follows:
In 2013, Lee, Che-Wei, and Wen-Hsiang Tsai [6] proposed a novel data hiding method for PNG images based on Shamir's (k, n)secret sharing scheme for color image authentication applications. In this method, the polynomial coefficients in Shamir's scheme are utilized as carriers for conveying the given data. The data to be hidden are transformed into partial shares, which are then embedded into the alpha channel plane of the cover PNG image. To alleviate the undesired white noise introduced by the data hiding process, the computed share values are carefully adjusted within appropriate ranges during embedding. In addition, an important application of the proposed method for color image authentication is presented, along with detailed algorithms for authenticating PNG images. Compared with existing methods, the proposed approach offers several advantages, including non-destructive authentication (the authentication process does not cause any modification or loss of the original image data, meaning that the image remains completely intact after authentication), high sensitivity to any image modifications, and an effective capability to locate tampered regions. Experimental results further demonstrate the effectiveness of the proposed approach for practical color image authentication applications.
In 2020, Sinhal, Rishi, Irshad Ahmad Ansari, and Chang Wook Ahn [7] proposed a blind fragile watermarking scheme (requiring no original image during recovery) for color images, aiming to achieve effective tamper detection and self-recovery. A pseudo-random binary sequence, generated based on a secret key, serves as a fragile watermark for tamper detection, while recovery information is stored randomly using a separate secret key. During embedding, each channel of the RGB image is divided into non-overlapping 2×4 blocks, and the watermark is embedded in each block using a Least Significant Bit (LSB) replacement technique according to a 9-rule coding structure. The watermark sequence for each block (12 bits) consists of 6 bits for tamper detection, coupled with 6 bits representing the Most Significant Bits (MSBs) of the average value of another block, contributing to image recovery in case of tampering. Experimental results demonstrate the high efficiency of the system in accurately identifying tampered regions with up to 99% accuracy, and a recovery capability of up to 80% even under severe modifications. Comparative evaluations confirm the superiority of this system over existing methods in terms of accuracy and performance.
In 2022, Wu, Hsien-Chu, et al**.** [8] proposed a model that combines convolutional neural networks with traditional digital watermarking techniques (DWTs), in which data integrity is ensured using a conventional authentication scheme within the discrete wavelet transform (DWT) domain. The effectiveness and performance of the proposed approach were investigated against several of the most common image tampering attacks. In addition, a comparison was conducted between the proposed approach and a number of recent works in this field. Experimental results demonstrate that this method provides a high capability for tampering detection. Moreover, the proposed approach is able to accurately recover the tampered regions in the image.
In 2022, Rezaei, Mehdi, and Hassan Taheri [9] proposed a novel scheme based on convolutional neural networks (CNNs) for image tampering detection and self-recovery, with a focus on protecting digital images against forensic tampering operations. To achieve this goal, the watermarking

 ISSN:2302-8149
e-ISSN:2540-9719

algorithm is required to possess two main properties: first, detecting the tampered regions in the received image using an authentication watermark; and second, recovering the tampered regions based on a watermark dedicated to the image digest. For tampering detection, a method for generating the authentication watermark based on a CNN is proposed, while the image digest is generated using the discrete cosine transform (DCT) and the JPEG quantization table. To compress the image digest and improve the quality of tampered region recovery, a comprehensive CNN-based compression framework is employed. In addition, the compressed image digest is encoded using Reed–Solomon error correction codes to protect it against high tampering rates. Finally, the Arnold transform is utilized to embed both the authentication watermark and the image digest watermark into the original image, thereby enhancing the security level. To demonstrate the performance of the proposed scheme, extensive experiments were conducted. Precision and Recall metrics were calculated to evaluate tampering detection performance, while PSNR and SSIM values were computed to assess image recovery quality. Comparisons with state-of-the-art methods indicate that the proposed scheme outperforms existing approaches in aspects such as security and recovery capability.

In 2024, Che-Wei Lee [10] proposed a novel distortion-free color image authentication method based on secret sharing, data compression, and image interpolation, with data recovery capability. The proposed approach generates carefully designed authentication signals serving two main functions: tamper localization and image restoration. The authentication signals are converted into multiple shares using a (k, n) threshold scheme, increasing the multiplicity of authentication signals and enhancing tamper recovery capability. These shares are then randomly embedded into the alpha channel of the protected image, which is converted to a PNG format supporting RGBA channels. During the authentication process, the extracted authentication signals from the alpha channel are used not only to detect tampering in image blocks but also as cues to retrieve the corresponding color from a predefined color palette, allowing recovery of tampered regions. Compared to recent methods, the proposed approach offers positive features, including lossless image quality, precise tamper localization, and efficient recovery of damaged regions. Finally, experimental results are presented, along with discussions on security considerations and comparisons with related methods, demonstrating the superiority of the proposed scheme.

Amrullah, Agit, et al. [11] In 2024 proposed a two-stage tamper detection mechanism for semi-fragile image watermarking using a two-level Integer Wavelet Transform (IWT). The study introduces a two-stage detection process to achieve high precision in tamper localization. In the first stage, the image is divided into four segments to determine whether any contains a tampered bit; a segment is classified as tampered if it contains at least one corrupted bit. The second stage is initiated only if the first stage reveals no tampering, conducting a fine-grained analysis of each segment. Furthermore, the study utilizes the Normalized Hamming Similarity (NHS) metric to classify malicious attacks. The proposed scheme applies a two-level IWT to decompose the image into LL, LH, HL, and HH sub-bands. Authentication bits from the LL sub-band are embedded into the LH and HL sub-bands to produce the watermarked image. For tamper localization, the LH and HL sub-bands are compared with the authentication bits using the bitwise XOR operation. Experimental results demonstrate that the proposed scheme achieves high reconstructed image quality, with an average PSNR of 44.1864 dB and an SSIM score of 0.9945. Moreover, the proposed method achieved a high tamper detection accuracy of approximately 98.33% under object manipulation attacks, with a tampering rate of approximately 12.1643%.

Vaidya, S. Prasanth, et al. In 2025 [12] developed an innovative fragile watermarking technique for image tamper detection and recovery, thereby enhancing the security of digital image transmission. The proposed method integrates Schur decomposition with the Discrete Wavelet Transform (DWT) for watermark embedding, ensuring superior robustness and resistance against attacks compared to existing methods. Schur decomposition provides numerical stability in matrix analysis, while the DWT enhances resilience through multi-resolution analysis. The semi-blind extraction algorithm, which relies solely on a secret key, enables active tamper detection without the need for the original image. Upon detecting distortions, the proposed recovery mechanism intervenes to reconstruct the tampered regions within the image. The efficacy of the proposed scheme was validated using Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), and Normalized Cross-Correlation (NCC) metrics, demonstrating superior performance over current approaches. This

 ISSN:2302-8149
e-ISSN:2540-9719

approach is applicable in fields such as secure medical imaging, digital forensics, and copyright protection, ensuring the integrity and reliability of images in real-world scenarios.
Now after surveying the existing literature on color image authentication and recovery, several studies were identified as major contributions in this field. These works are reviewed with respect to the employed techniques, along with their corresponding advantages and limitations, as summarized in Table 1.

Table 1 show techniques used, advantages and disadvantages

author	techniques used	advantages	disadvantages
Lee, Che-Wei, and Wen-Hsiang Tsai (2013).[6]	Data hiding method relies on secret sharing of information via PNG images for color image authentication applications.	Non-destructive authentication, i.e., the image verification process does not result in any change or loss of the original image data, high sensitivity to any image modifications, and effective ability to locate tampering area.	For authentication purposes only and the data has not been recovery and repair. It was not tested for resistance against Sequential Composite Attacks
Sinhal, Rishi, Irshad Ahmad Ansari, and Chang Wook Ahn (2020).[7]	A new method for detecting fragile watermarks in color images to detect alterations and restore images	Detect modifications and locate any changes made to the image. Restore the original image even if it has been severely modified up to 80%.	It depends on the modification of the cover image. Restoration accuracy is lost in images with significant contrast between adjacent pixels, especially in cases of minor manipulation. As the degree of manipulation increases, the quality of the restored image deteriorates. It was not tested for resistance against Sequential Composite Attacks
Wu, Hsien-Chu, et al (2022).[8]	A methodology and model that combines convolutional neural networks with fragile digital watermarking techniques in the discrete wavelet transform (DWT) domain.	A novel approach for grayscale image authentication that enables tamper localization and recovery, with convolutional neural networks enhancing the quality of restored images.	The approach relies on modifications to the cover image. It is limited in terms of the size and types of tampering that can be recovered. The methodology was applied exclusively to grayscale images, with no use of color images. It was not tested for resistance against Sequential Composite Attacks.
Rezaei, Mehdi, and Hassan Taheri (2022).[9]	A novel approach based on convolutional neural networks (CNNs) and watermarking for image tampering	A robust methodology for grayscale image authentication and recovery, characterized by effectiveness in terms of accuracy and the ability to	The approach depends on modifications to the cover image. It is limited regarding the size and types of tampering that can be restored. Furthermore, applying the method to scanned documents and color images

 ISSN:2302-8149
e-ISSN:2540-9719

	detection and self-recovery.	detect potential modifications while preserving image quality.	poses challenges that have not yet been addressed. It was not tested for resistance against Sequential Composite Attacks.
Che-Wei Lee (2024). [10]	A distortion-free authentication method for color images with tampering localization and self-recovery	The image verification process results in no alteration or loss of the original image data, as the authentication signals are embedded in the alpha channel. It features high-performance color image authentication, high accuracy in detecting tampering, and self-repair capabilities.	Limitations in the extent and type of tampering that can be corrected, in addition to the complexity of implementation. Reliance on a specific color palette, as it relies on a pre-defined color palette, which may limit its flexibility in handling images with diverse colors. In addition, the method faces challenges in applying it to color scanned documents, as it relies on color changes (color details) to identify tampering, making it less effective with other documents Due to the nature of documents that rely on text and fonts rather than color details. It was not tested for resistance against Sequential Composite Attacks
Amrullah, Ernawan, Raffei, Chuin (2024).[11]	A Two-Stage Tamper Detection Mechanism for Semi-Fragile Image Watermarking Using Two-Level Integer Wavelet Transform (IWT)	The proposed methodology achieves high-precision tamper localization with the capability of recovering the corrupted image, while maintaining the host image quality after watermark embedding. Furthermore, it ensures a high security level for the watermark data, as both authentication and recovery information are encrypted using the Multiple Scrambling technique	Despite its effectiveness, the methodology exhibits limitations regarding the precision of tamper detection. There are constraints on the scale and nature of the recoverable distortions, as the approach shows a clear vulnerability to text-insertion attacks on the image. Additionally, the performance was primarily evaluated under low-intensity damage scenarios. Furthermore, the methodology relies on direct modifications to the cover image and has been limited to grayscale images, without extension to color image formats. The methodology has not been evaluated against sequential composite attacks

 ISSN:2302-8149
e-ISSN:2540-9719

Vaidya, Kandala, et al (2025) [12]	A Robust and Fragile Digital Watermarking Approach for Image Tamper Detection and Recovery Using Hybrid Transforms"	The proposed methodology achieves high accuracy in both tamper detection and localization, alongside the capability to recover corrupted images. By incorporating the [insert algorithm name here] clustering algorithm, the efficiency of restoring damaged image regions has been significantly enhanced. Furthermore, the approach achieves an effective integration of authentication and recovery data within the host image.	The proposed methodology has several identified limitations. First, it relies on direct modifications to the host image, which may affect its original integrity. Second, the current implementation is restricted to grayscale images, without support for color imagery. Third, there are inherent constraints regarding the scale and nature of the tamper that can be effectively recovered. Finally, the methodology involves significant computational complexity; while the utilization of 4x4 blocks enhances localization precision, the extensive subdivision of the image combined with the processing of Discrete Wavelet Transform (DWT) coefficients leads to a notable increase in the overall computational overhead of the system. The methodology has not been evaluated against sequential composite attacks

The main contributions of this study are summarized as follows:
Extending the Previous Methodology: Enhancing our earlier framework by integrating a secret sharing scheme with alpha layer embedding and spatial correlation to handle advanced image manipulation scenarios.
Addressing Sequential Composite Attacks: Proposing a robust solution for a previously unexplored domain in the literature, where the framework is rigorously evaluated under complex and successive combined attacks.
Superior Performance and Reliability: Demonstrating exceptional tamper detection and image restoration capabilities while maintaining high visual quality for both stego and recovered images (validated via PSNR and SSIM metrics).

3. Methodology:

3.1 Overview:

The methodology employed in this study is identical to the one previously published [4], relying on the extraction of the five most significant bit planes from each color channel of the image, resulting in a total of fifteen-bit planes. Subsequently, fifteen secret bit planes are generated using Shamir's Secret Sharing scheme, and these secret data are embedded into the alpha layer for the authentication and recovery of color images. The primary objective of the current research is to extend the application of this methodology to address the challenges posed by sequential composite attacks, without introducing any modifications to the original algorithm.

In traditional single-attack scenarios, authentication data localized in specific regions may either survive or fail. However, sequential composite attacks (such as a spatial attack followed by signal processing) often completely destroy localized recovery data. Our extended approach leverages the mathematical properties of Shamir's Secret Sharing combined with non-contiguous spatial block correlation within the alpha layer. This ensures that even if a primary manipulation corrupts a portion of the stego image, the remaining shares distributed across unaffected or partially affected blocks retain sufficient mathematical integrity to reconstruct the secret and

 ISSN:2302-8149
e-ISSN:2540-9719

successfully recover the image. Furthermore, the validation framework was systematically engineered to simulate multi-stage degradation (worst-case composite scenarios) rather than isolated incidents. By testing successive combinations of spatial and non-spatial distortions, we rigorously proved that the interaction between alpha channel embedding and secret sharing maintains mathematical convergence, preventing catastrophic failure during multi-step tampering.

3.2 Summary of the Original Methodology:

The original approach consists of the following key steps:

authentication data embedding process:

Figure1 illustrates the details of the authentication data embedding process

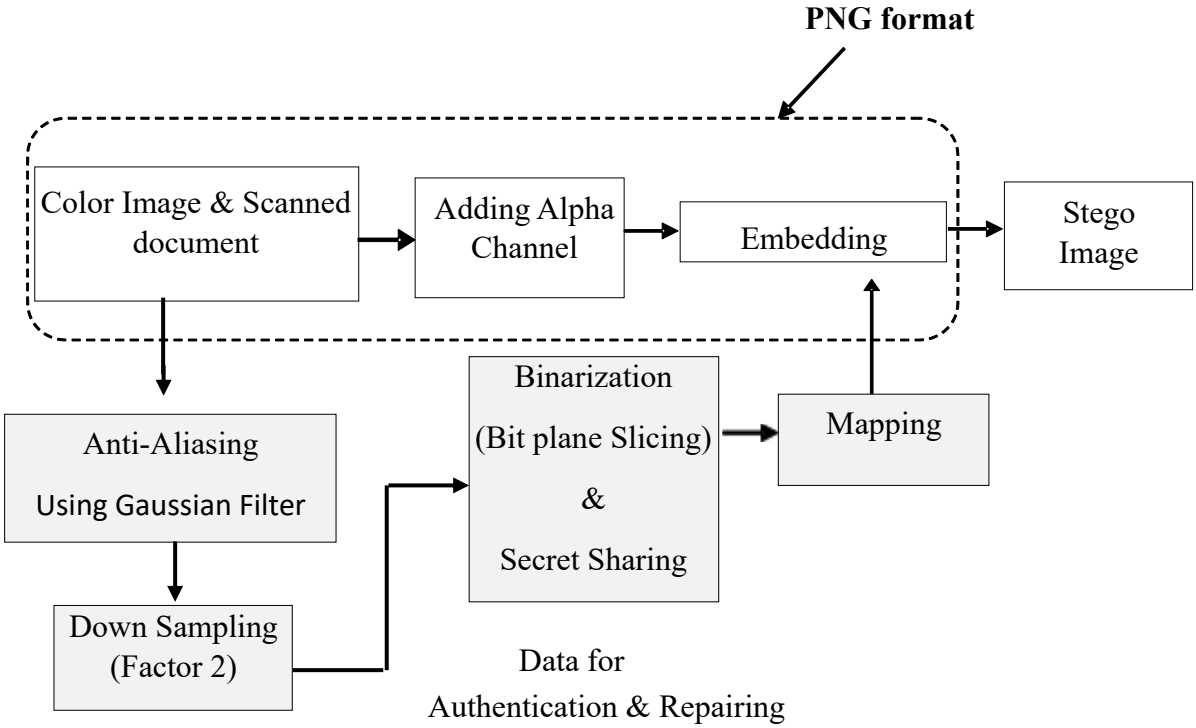


Figure 1 authentication data embedding process [4]

Stego Color Image Authentication and Verification:

Figure2 illustrates the details of the Stego Color Image Authentication and Verification:

 ISSN:2302-8149
e-ISSN:2540-9719

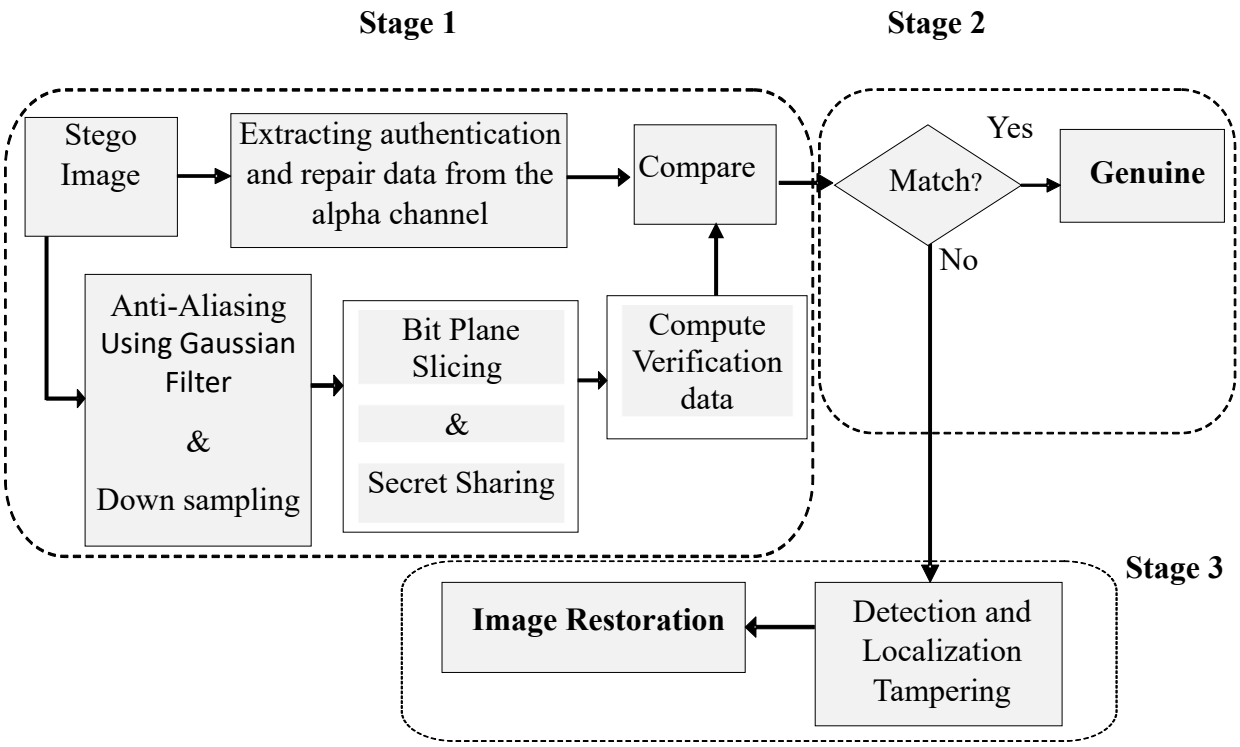


Figure 2 authentication process that involves verifications and self-repairing a color PNG image [4]

While this study builds upon the foundational architecture of our previous framework, its primary scientific contribution does not lie in developing a new embedding algorithm from scratch, but rather in fundamentally extending its capability and structural resilience to confront an unaddressed challenge in the literature: Sequential Composite Attacks. Unlike our earlier work which focused on evaluating system performance under isolated, single-attack scenarios (e.g., individual cropping or noise addition) the current study introduces a targeted spatial correlation and secret-sharing adaptation designed to withstand multi-stage, cascading degradations. Consequently, the core originality of this work resides in the rigorous validation and behavioral analysis of the framework under worst case composite scenarios, proving mathematically and experimentally that distributed alpha layer embedding can prevent catastrophic failure where traditional single-attack paradigms fail.

3.3 Expanded Application:

Sequential Composite Attacks:

Sequential Composite Attacks are defined as attacks involving multiple successive manipulations applied to a single image, such as cropping followed by Gaussian noise addition, text attacks followed by salt-and-pepper noise, or superimposition followed by enhancement attacks. These attacks present a more complex challenge compared to conventional single attacks, as the tampering becomes cumulative and more difficult to detect.

In this study, the original methodology is evaluated under sequential composite attacks to assess its robustness. The evaluation is conducted using standard image quality metrics, including Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), among other quality measures. Additionally, the effectiveness of tamper detection and image recovery is assessed.

 ISSN:2302-8149
e-ISSN:2540-9719

As sequential composite attacks on color image authentication and recovery remain an unexplored domain in current literature, no direct counterparts exist for comparison. To rigorously assess our approach, validation is performed through the practical implementation of the methodology and its evaluation against a diverse range of potential sequential composite attacks.

4. Results

In this section, we present the simulation results to evaluate the performance and effectiveness of the developed algorithm against sequential composite attacks for the authentication of color images and scanned color documents, as well as the capability for data recovery.

In this study, full-reference IQA metrics were used to analyze the algorithms' performance [4]-[13]-[14]-[15]. The following FR-IQA parameters were used for evaluation:

Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Average Difference (AD), Structural Similarity Index Measure (SSIM), and Structural Content (SC). In addition, two additional parameters were calculated to evaluate the proposed algorithm:

Embedding Capacity (EC) and Number of Embedded Bits (NBE).

4.1 Embed authentication and recovery data:

A real-world color document image of the "Adhar" will be used as the cover image for the test application. This color image size is 1112 x 700. An alpha channel will be added to this cover image, and the authentication and repair data will be embedded in the alpha channel as follows:

(a)

 ISSN:2302-8149
e-ISSN:2540-9719

(b)

(c)

Fig 3 Embed authentication data Process of color Image (a) Cover Image

(b) Alpha Channel + Authentication Data (c) Stego image

The quality parameters for the above embedding process were calculated. These calculated parameters are shown in Table 2:

Table 2 quality parameter values for color Image

Image Quality Parameter Color document image	Values
Stego Color Image PSNR in dB	100
Alpha Channel PSNR in dB	34.2165

 ISSN:2302-8149
e-ISSN:2540-9719

Image Quality Parameter Color document image	Values
Alpha Channel MSE	24.628
Alpha Channel SC	0.978781
Alpha Channel AD	2.75375
Alpha Channel NCC	0.999884
Alpha Channel EC	6227200
Alpha Channel NBE	3113600

4.2 External Sequential Composite Attacks on Stego color Image, Authenticity verification and data recovery:

Digital color images are attacked in a variety of ways and techniques. Our study will focus on tow Sequential Composite Attacks that distort and alter the actual content of an image and affect the visual quality of the image. These attacks include:

1) Cropping attack followed by Gaussian noise
2) text attack followed by salt-and-pepper noise
3) superimposition attack followed by Cropping attack followed by enhancement attack

1) cropping followed by Gaussian noise:

in first attack, the face of the person in the color image will be cropped to hide landmarks and identity. Figure 4 shows the cropped image:

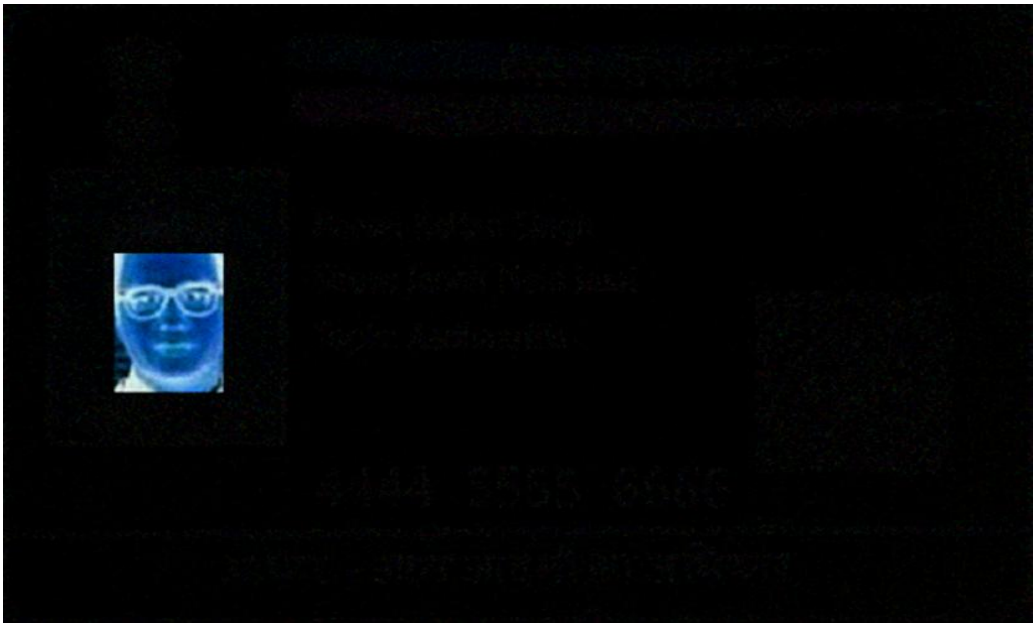
Figure 4 first attack, Cropping attack on color Image

The second attack is Gaussian noise. Figure 5 shows the Gaussian noise attack on color image:

 ISSN:2302-8149
e-ISSN:2540-9719

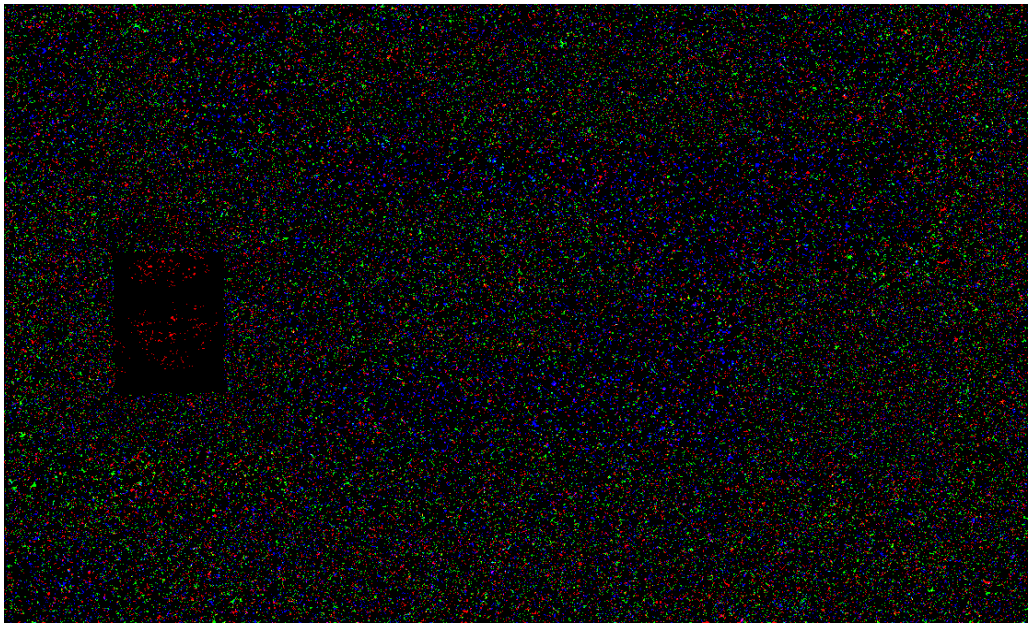
Figure 5 Second Attack, Gaussian Noise Attack On Color Image

Now we will perform the authentication, verification and data recovery process for the color image after this tow Sequential Composite Attacks.



(a)

 ISSN:2302-8149
e-ISSN:2540-9719



(b)

(c)

Figure 6. Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 6 shows the detailed results of the authentication and data recovery. Figure6(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure6 (b) shows the identification of the tampered region, and Figure 6(c) is the repaired image. This image is obtained by matching the authentication data with the tampered region.

The quality parameters of the repaired and restored color image were calculated and are shown in Table 3:

Table 3 quality parameters for color Image for cropping attack and Gaussian noise attack

Image Parameter (Quality) Color document Image	Values
PSNR (dB)	31.6334

 ISSN:2302-8149
e-ISSN:2540-9719

Image Parameter (Quality) Color document Image	Values
MSE	41.0633
NCC	0.999676
SC	0.972995
AD	3.01472
SSIM	0.917918

2) Text attacks followed by salt-and-pepper noise:

in first attack, an external text is embedded into the colored document image with the purpose of claiming ownership of this image. Figure 7 shows the Text Attack on the Color Document Image:

Figure 7 first attack, Text attacks on color Image

The text 'Maher Al Dbsawie' was inserted into the image with the intention of falsely claiming its ownership. The second attack is salt-and-pepper noise. Figure 8 shows the Gaussian noise attack on color image:

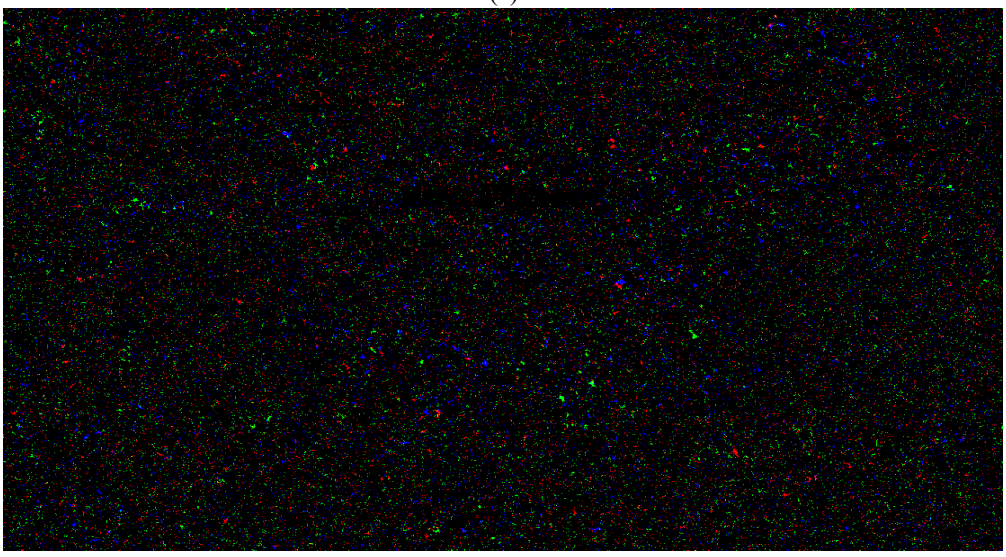
Figure 8 second attack, salt-and-pepper noise attack on color Image

In this attack, salt-and-pepper noise with a density of 0.2 was added. This implies that 20% of the total image pixels are affected, which produces a highly noticeable distortion.

 ISSN:2302-8149
e-ISSN:2540-9719

Now we will perform the authentication, verification and data recovery process for the color image after this tow Sequential Composite Attacks.

(a)



(b)

(c)

 ISSN:2302-8149
e-ISSN:2540-9719

Figure 9 Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 9 shows the detailed results of the authentication and data recovery. Figure 9(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 9(b) shows the identification of the tampered region, and Figure 9(c) is the repaired image. This image is obtained by matching the authentication data with the tampered region.

The quality parameters of the repaired and restored color image were calculated and are shown in Table 4:

Table 4 quality parameters for color Image for Text attacks and salt-and-pepper noise attack

Image Parameter (Quality) Color document	Values
PSNR (dB)	32.1808
MSE	35.3195
NCC	0.99974
SC	0.972171
AD	3.09784
SSIM	0.949527

3) superimposition attack followed by Cropping attack followed by enhancement attack

In this attack, there will be three sequential composite attacks. The first attack is a superimposition attack, in which a white rectangle is added to the color document image. Figure 10 shows the superimposition attacks:

Figure 10 first attack, superimposition attacks on color Image

The second attack is Cropping attacks. Figure 11 shows the Cropping attack on color image:

 ISSN:2302-8149
e-ISSN:2540-9719

Figure 11 second attack, Cropping attack on color Image

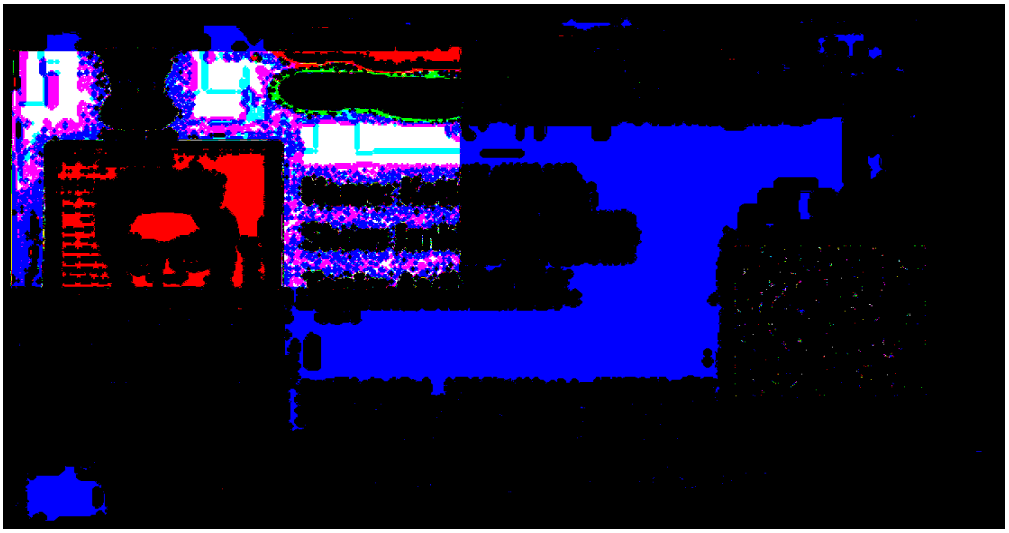
The third attack is an enhancement attack. Figure 12 shows the enhancement attack on color image:

Figure 12 third attack, enhancement attack on color Image

Now we will perform the authentication, verification and data recovery process for the color image after this tow Sequential Composite Attacks.

(a)

 ISSN:2302-8149
e-ISSN:2540-9719



(b)

(c)

Figure 13 Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 13 shows the detailed results of the authentication and data recovery. Figure 13(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 13(b) shows the identification of the tampered region, and Figure 13(c) is the repaired image. This image is obtained by matching the authentication data with the tampered region.

The quality parameters of the repaired and restored color image were calculated and are shown in Table 5:

Table 5 quality parameters for color Image for superimposition attack and Cropping attack and enhancement attack

Image Parameter (Quality) Color document Image	Values
PSNR (dB)	32.8435
MSE	32.8917
NCC	0.999743
SC	0.975403

 ISSN:2302-8149
e-ISSN:2540-9719

Image Parameter (Quality) Color document Image	Values
AD	2.77694
SSIM	0.957071

5. Conclusion

In conclusion, this paper successfully proposed and validated an extended framework for color image authentication and recovery utilizing the alpha layer, secret sharing, and noncontiguous spatial block correlation to effectively counter complex sequential composite attacks. The experimental results demonstrated outstanding performance recording high PSNR and SSIM values even under severe multi-stage tampering while preserving the visual quality of both stego and recovered images. This framework holds significant practical potential across sensitive domains such as digital forensics, electronic document security, and secure digital archiving. Building upon these promising outcomes, future work will focus on scaling the methodology to handle emerging sophisticated attack vectors, optimizing computational complexity for real-time video processing, and investigating the integration of lightweight machine learning techniques for enhanced tamper localization.

References

[1] Rathod, Subhash, and A. K. Gupta. "*An Authentication and Recovery Method for Color IMAGES*." (2014). http://inpressco.com/category/ijcet

[2] Reyes-Reyes, Rogelio, et al. "*Color Image Self-Recovery and Tampering Detection Scheme based on Fragile Watermarking with High Recovery Capability*." Applied Sciences 11.7 (2021): 3187. https://doi.org/10.3390/app11073187

[3] Al Dbsawie, Maher & Alasli, Soliman & Jabbouli, Hassan. (2024). *Advanced Authentication and Recovery in Grayscale Imaging via Alpha Layer and Secret Sharing*. Nanotechnology Perceptions. DOI:10.62441/nano-ntp.v20iS13.94

[4] Al Dbsawie, Maher Adel, Suleiman Alassly, and Hasan Al Jabbouli. "*A Novel Approach for Secure and Reliable Color Image Authentication and Recovery using Alpha Layer and Secret Sharing*." *Sistemasi: Jurnal Sistem Informasi* 15.6 (2026): 2057-2086. https://doi.org/10.32520/stmsi.v15i6.6340

[5] Al Dbsawie, Maher, Mohammed Amin Zabadani, and Hassan ALJabbouli. "*A High Payload Double Secured Video Steganography based on aes Encryption and bch Code*." *2021 IEEE International Conference on Computing (ICOCO)*. IEEE, 2021. DOI: 10.1109/ICOCO53166.2021.9673559

[6] Lee, Che-Wei, and Wen-Hsiang Tsai. "*A Data Hiding Method based on Information Sharing via PNG Images for Applications of Color Image Authentication and Metadata Embedding*." Signal Processing 93.7 (2013): 2010-2025. 10.1016/j.sigpro.2013.01.009

[7] Sinhal, Rishi, Irshad Ahmad Ansari, and Chang Wook Ahn. "*Blind Image Watermarking for Localization and Restoration of Color Images*." IEEe Access 8 (2020): 200157-200169. DOI: 10.1109/ACCESS.2020.3035428

[8] Wu, Hsien-Chu, et al. "*An Image Authentication and Recovery System based on Discrete Wavelet Transform and Convolutional Neural Networks*." *Multimedia Tools and Applications* 81.14 (2022): 19351-19375. https://doi.org/10.1007/s11042-021-11018-4

[9] Rezaei, Mehdi, and Hassan Taheri. "*Digital Image Self-Recovery using CNN Networks*." *Optik* 264 (2022): 169345. https://doi.org/10.1016/j.ijleo.2022.169345

[10] Lee, Che-Wei. "*A Distortion-Free Authentication Method for Color Images with Tampering Localization and Self-Recovery*." Signal Processing: Image Communication 124 (2024): 117116. 10.1016/j.image.2024.117116

[11] Amrullah, Agit, et al. "TDSF: *Two-Phase Tamper Detection in Semi-Fragile Watermarking using Two-Level Integer Wavelet Transform*." *Engineering Science and Technology, an International Journal* 61 (2025): 101909. https://doi.org/10.1016/j.jestch.2024.101909

[12] Vaidya, S. Prasanth, et al. "*A Robust Fragile Watermarking Approach for Image Tampering Detection and Restoration Utilizing Hybrid Transforms*." *Scientific Reports* 15.1 (2025): 17645. https://www.nature.com/articles/s41598-025-01297-4

[13] Mustafa, Wan Azani, et al. "*A Review of Image Quality Assessment (IQA): Snr, gcf, ad, nae, psnr, me*." Journal of advanced research in computing and applications 7.1 (2017): 1-7.

[14] Hisham, M. B., et al. "*Template Matching using Sum of Squared Difference and Normalized Cross Correlation*." 2015 IEEE student conference on research and development (SCOReD). IEEE, 2015. https://doi.org/10.1109/SCORED.2015.7449303

[15] Wang, Zhou, et al. "*Image Quality Assessment: From Error Visibility to Structural Similarity*." IEEE transactions on image processing 13.4 (2004): 600-612. https://doi.org/10.1109/TIP.2003.819861