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

A Novel Approach for Secure and Reliable Color Image Authentication and Recovery using Alpha Layer and Secret Sharing

[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*:** 17 April 2026, ***revised*:** 15 June 2026, ***accepted*:** 24 June 2026)

Abstract

In the contemporary digital environment, securing digital images against forgery has become a critical necessity, particularly in sensitive domains such as the judiciary, criminal investigations, and communications security. Any manipulation or falsification of legal documents or digital evidence can lead to serious consequences and significant challenges. This study proposes a method for protecting color scanned images and documents by utilizing an invisible component within them, specifically the alpha channel (transparency layer), to embed authentication and recovery data. The process begins by applying a Downsampling operation to the cover image to reduce its size while preserving fine visual details, taking into account the removal of aliasing to achieve the best possible representation of edges and details prior to reduction. Subsequently, 15 secret bit planes are combined to form 4 composite secret bit planes, which are then embedded into the alpha channel. During the recovery phase, these four bit planes are extracted from the alpha channel, from which the original 15 authentication bit planes are reconstructed. The reconstructed data are then matched with the verification data, and in case of any discrepancy, the image is repaired using the embedded authentication data. This approach enables the detection of any tampering and facilitates image recovery if it has been altered or manipulated. One of the key advantages of this method is that it does not affect the visual quality of the host image, as the data are embedded within the added alpha channel. Any attempt to tamper with the image can be detected, and based on the embedded data, the modified or deleted regions can be restored. The proposed method was tested on various types of color scanned images and documents under diverse attack scenarios (content modification attacks and visual quality attacks), demonstrating remarkable effectiveness in preserving image integrity. This technology is particularly important for law enforcement, information security, digital forensics, and any security teams requiring reliable image authentication. The system is also designed to be user-friendly and does not require any specialized hardware, making it practical and suitable for real-world applications.

Keywords: Authentication, Data Hiding, Watermarking, Tamper Detection, Data Recovery, secrete sharing, Alpha channel, color image.

1. Introduction

The integrity and authenticity of digital images are critical concerns in domains such as medicine, legal documentation, and national security, where the slightest manipulation can lead to severe consequences. For instance, a tampered medical image may result in an incorrect diagnosis, while a forged legal document can lead to miscarriage of justice. As digital images become increasingly prevalent, the demand for secure and reliable image authentication and recovery mechanisms continues to grow. Conventional watermarking and authentication techniques typically

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

involve embedding verification data directly into the image content. However, this often leads to visible distortion or degradation of image quality, especially when fragile watermarking is required for tamper detection [1][2]. To address this trade-off between invisibility and robustness, recent studies have proposed utilizing the alpha channel an often-underused component in color images to embed authentication data [3]. This channel enables hidden data embedding without compromising the visual appearance of the image, thus preserving its perceptual quality. Achieving strong authentication of digital images requires seven important variables through which the effectiveness of the authentication system is evaluated [4-8]:

• Sensitivity: The authentication system must be able to detect any changes or tampering with the material. Detecting any modification, not just content modification, is also required for strong authentication methods.
• Robustness: Tolerance is another word for robustness. The authentication system must tolerate content-preserving modifications. Only algorithms that offer selective authentication are eligible for this feature.
• Localization: The authentication system must be able to identify altered locations and regions in the image.
• Recovery: The authentication system must be able to recover regions of the image that have been partially or completely altered.
• Security: The authentication system must be able to protect the authentication data from any attempts at tampering or alteration.
• Portability: During any transmission, storage, or processing activity, the authentication system must be able to transmit the signature in the protected image.
• Complexity: The authentication system should rely on real-time methods that are not complex or slow.

In this research, we propose a novel framework for secure and reliable authentication and recovery of color images by combining the alpha channel with a secret sharing scheme, as introduced by Shamir [9]. Secret sharing is a powerful cryptographic technique that divides a secret into multiple parts (or shares), requiring a minimum number of shares to reconstruct the original information. By embedding these shares into the alpha channel, we ensure that even if a portion of the image is tampered with or lost, the original image content can be accurately verified and restored. The proposed method performs two key functions: (1) detecting any unauthorized modification in the image, and (2) enabling recovery of the altered regions by reconstructing the authentication data from the embedded shares. Experimental results demonstrate that the approach offers high imperceptibility, strong tamper detection sensitivity, and effective recovery capability against common image attacks such as noise, cropping, and modifications. This makes our system particularly suitable for real-world applications where image integrity is of critical importance.

2. Literature Review

Most studies in the current literature focus on authenticating binary and grayscale images [10–11–12–13]. In contrast, color images do not receive the same level of attention, particularly with regard to restoration processes. While authenticating color images is relatively straightforward, restoring their data poses a greater challenge due to the need to recover a large amount of pixel information across the red, green, and blue channels.

After reviewing some of the available literature on the authentication and recovery of both grayscale and color images, several papers have emerged as significant contributions in this field. These papers will be analyzed in terms of the techniques used, as well as their advantages and disadvantages, as presented in Table 1.

Table 1 show techniques used, advantages and disadvantages

author	techniques used	advantages	disadvantages
Arya, K. V., and Akanksha Bandil (2014)	Grayscale image authentication and data restoration	The image and the data contained within it, being in grayscale PNG format, are self-	As it cannot withstand potential attacks or modifications. There are limitations on the types of attacks it

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

[14]	using the PNG format	repairable	can tolerate. The color image was not used.
Lee, Che-Wei, and Wen-Hsiang Tsai (2010) [15]	Authentication of binary document images in PNG format based on secret sharing technology	The image and the data contained within it, being in grayscale PNG format, are self-repairable	The color image was not used. The system focuses specifically on grayscale source document images. Potential attacks or modifications cannot be resisted.
Nichal, Arjun, and Bhalchandra Godbole (2021) [16]	An effective method and methodology for authentication with data restoration capability for grayscale images, based on bit-level slicing and embedding authentication data into the channel	Detecting modifications and locating any change or tampering made to the image. The ability to recover the original image even if it has been subjected to modifications	The methodology focuses specifically on grayscale images without addressing grayscale scanned documents. Limitations in the size and type of tampering that can be repaired. This methodology relies on embedding explicit data into the image's alpha channel. This embedding poses a security challenge, as the embedded original data must be secured against detection or tampering. The color image was not used.
Wu, Hsien-Chu, et al (2022) [17]	A methodology and model that combines convolutional neural networks and fragile digital watermarking techniques in the transform domain (DWTs)	A distinctive approach to achieve authentication for grayscale images with the ability to locate tampering and manipulation, as well as repairability, where the convolutional neural network helped improve the accuracy of the restored images	It relies on modifying the cover image. Limitations in the size and type of tampering that can be repaired. The methodology was applied only to grayscale images, and color images were not used
Rezaei, Mehdi, and Hassan Taheri (2022) [18]	A novel approach based on convolutional neural networks (CNNs) and watermarking for detecting image tampering and self-recovery	A robust methodology for authentication and restoration of grayscale images, characterized by effectiveness in terms of accuracy and the ability to detect possible modifications to the image while maintaining image quality	It relies on modifying the cover image. Limitations in the size and type of tampering that can be repaired. In addition to challenges in applying the method to scanned documents and color images, which were not addressed
Lee, Che-Wei, and Wen-Hsiang Tsai (2013).[19]	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.

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

Sinhal, Rishi, Irshad Ahmad Ansari, and Chang Wook Ahn (2020).[20]	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.
Nichal, Arjun, and Bhalachnadra Godbole (2021).[21]	An effective method and methodology for authentication with the ability to recover color image data is based on bit-Plane slicing and the inclusion of authentication data in the alpha channel.	Detects modifications and identifies any changes or manipulations made to the color image. The original image can be recovered even if it has been modified or tampered with.	The methodology focuses specifically on color images, excluding color scanned documents. There are limitations in the size and type of manipulation that can be rectified. This methodology relies on embedding explicit data in the image's alpha channel. This embedding poses a security challenge, as the embedded original data must be secured against detection or tampering.
Che-Wei Lee (2024). [22]	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.
Molina-Garcia, Javier, et al [23]	A Fragile Watermarking Scheme for Color Image Authentication and Self-Recovery	The watermarked images exhibit higher quality, and the proposed scheme is capable of reconstructing highly tampered regions (up to 80%) while achieving good quality for the tampered and self-recovered areas, in addition to providing better visual performance compared with a similar scheme from state-of-the-art methods.	It depends on modifying the cover image. There is a limitation in the type of tampering that can be repaired. As the tampering ratio increases, the quality of the recovered image degrades significantly. In addition, there are challenges in applying the method to color scanned documents, which have not been addressed.

After reviewing the various methods used for authentication and data repair, the following observations were identified:

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

• In most authentication techniques, authentication data is embedded within the image data itself rather than within the host file. This may affect the visual quality of the image and makes it more vulnerable to loss or tampering.
• Most algorithms proposed in the literature focus solely on the authentication aspect, without providing effective mechanisms for data recovery or restoration in cases of tampering or corruption.
• In most techniques, the host image suffers from a reduction in visual quality after embedding authentication data, which limits the effectiveness of these methods in quality-sensitive environments such as official documents or medical images.
• The ability to repair tampered or modified image data remains limited. Most current studies focus on grayscale and binary digital images and their recovery, without adequately addressing color images and documents. The fundamental challenge in repairing scanned digital documents lies not only in recovering text or visual elements but also in restoring visual homogeneity. This requires effective techniques that consider color gradations and align with human visual perception.
• Large-scale images and documents present an additional challenge, unlike the standard 512×512 pixel images commonly used in studies and techniques. This challenge is further intensified when dealing with color scanned images and documents due to storage and processing requirements.
• The diversity of studied attacks is limited; some studies focus only on content modification attacks, while others address attacks affecting visual image quality.
• In some methodologies, explicit data is embedded within the alpha layer, which poses a security risk to the authentication system in terms of potential data forgery, modification, or identification. Therefore, a high level of security and robustness must be achieved in protecting the embedded authentication and repair data to ensure strong resistance against tampering attempts or malicious attacks targeting this data.

- **Definition of objectives:**

1- Building and developing an effective system for authenticating color scanned images and documents, aiming to verify content authenticity and determine whether it has been modified or tampered with.
2- Accurately detecting the locations of modifications or tampering that may be performed on color images or documents, in order to provide a higher level of reliability in authentication.
3- Embedding and integrating authentication data within the host image instead of storing it in a separate data file or embedding it directly into the image data in a way that may affect the host image quality, thereby enhancing integrity, security, quality, and usability.
4- Enabling the proposed system to perform effective mechanisms for recovering original data in the event of detected changes or partial damage, thus enhancing system reliability in terms of self-repair of content.
5- Preserving the visual and perceptual quality of the original content after embedding, through precise techniques that ensure images and documents remain usable and displayable without distortion or loss of details.
6- The proposed system must ensure the protection of embedded authentication and recovery data against tampering or forgery attempts, while maintaining their accurate recoverability under common processing operations, by achieving a balance between security and robustness.
7- The proposed system must achieve the required balance between sensitivity and robustness, ensuring the ability to detect subtle malicious modifications that may occur in color scanned images or documents, while maintaining resistance to unintended changes or common processing operations.

3. Methodology

This system proposes a secure and reliable method for authenticating color images with the possibility of data recovery and repair. The system includes two algorithms: the first is an authentication data embedding algorithm and the second is a data extraction and verification algorithm [24]. The proposed method first converts the cover color image and scanned document to

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

the Portable Network Graphics (PNG) format by adding an alpha channel to it. Meanwhile, the five most significant levels from the three-color channels (R, G, and B) are taken for authentication and data repair. The contributions of these levels are then calculated, and the data is embedded in the alpha channel while maintaining the highest level of transparency. The Stego image is generated in PNG format. The authentication data embedding process involves the following steps. Figure1 shows the stage of the authentication data embedding process.

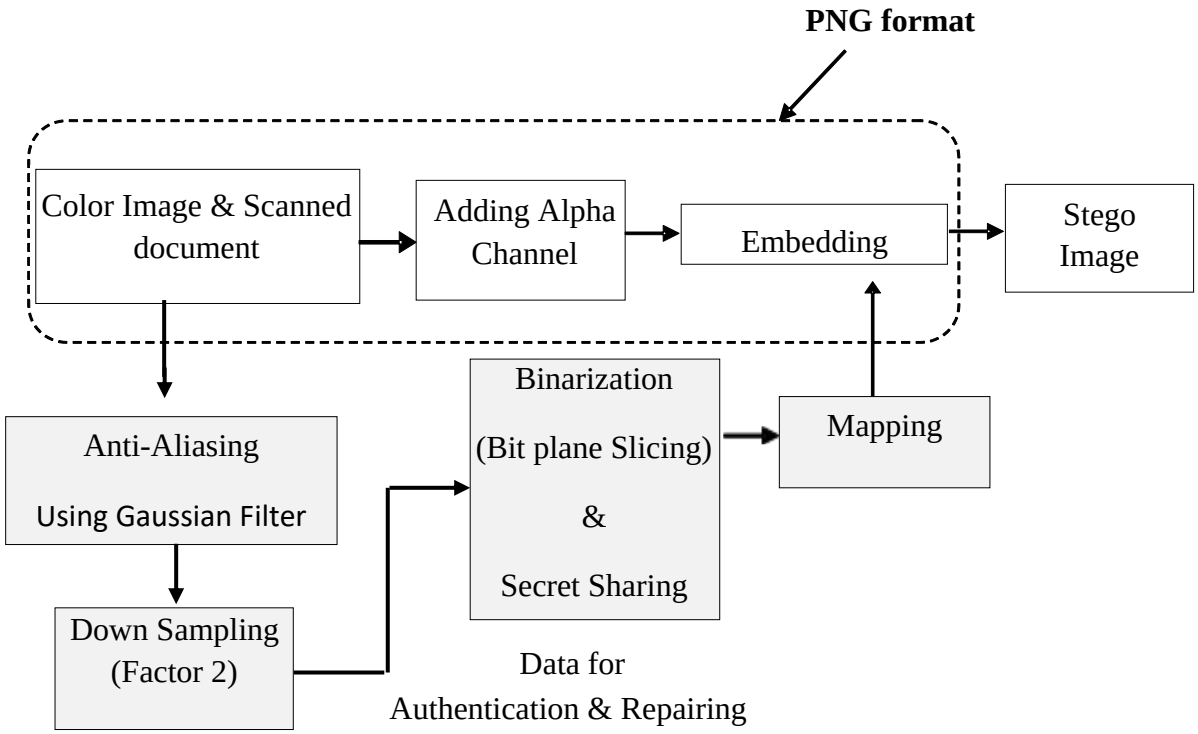


Figure 1 authentication data embedding process

3.1 Creation of the Stego Image

Step 1: Cover Image

The selected color input image is a 24-bit image. It has extensions of PNG, JPG, BMP, etc. The color image is represented in the following format:

Let I denote the input color image of dimensions m x n x cp. The image I can be mathematically represented as equation (1):

$$I = \{x(i,j,k) \mid 1 \le i \le m,\ 1 \le j \le n,\ 1 \le k \le cp,\ x(i,j,k) \in \{0,1,2,\dots,255\}\} \quad (1)$$

where m and n represent the height and width of the image respectively, and cp denotes the number of color channels. The term full color image is often used to refer to a 24-bit RGB color image [25].

Step 2: Adding an Alpha Channel

At this stage, the alpha channel is constructed. This is the fourth layer of the image. The resulting image will be a color image. There are three channels in the color image. For transparency, an alpha channel is added to the image. Repairing self-manipulated data in the affected image areas contrasts with the fact that the cover image is first destroyed, and the original data is no longer available for repair. This occurs after the original cover image data is embedded in the image itself for use in subsequent data recovery. One way to address this problem is to copy the original image data elsewhere without altering the cover image itself. This study proposes using an additional alpha channel of a PNG image to contain the original image data to achieve this technique. However, the alpha channel of the PNG image was initially used to provide the appropriate level of transparency. Furthermore, embedding the data in the alpha channel would result in an unwanted opaque effect and unexpected transparency in the PNG image. Binding the resulting values to a limited range around its maximum value of 255 could make the alpha channel level nearly invisible. One way to achieve the desired result is this. This is how an alpha channel is defined as equation (2) [26].

(2)

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

$$Alpha = \left\{ a(x,y) \;\middle|\; \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y) = 255 \end{matrix} \right\}$$

Step 3: Color image down sampling with a down sampling factor 2:
In this step, the size of the input image is reduced so that we get a thumbnail. The down sampling is done by 2, which naturally reduces the size of the original data. We performed this process because the proposed algorithm has one limitation: the data required for authentication is large. To hide 15 bit levels of secret shares (5 bit planes for red, 5 bit planes for green, and 5 bit planes for blue) in an 8-bit alpha channel, the cover image size must be reduced. For example, let's assume the input cover image size is 1024x1024. After applying down sampling by 2, the image size will change to 512x512. This process is illustrated in Algorithm.1 as follows:

Algo. 1: Anti- Aliasing and Down sampling of Input color image with factor 2

Input: Cover color image

Output: Scaled-down color image

Step 1: Cover color image selection process
Step 2: Doing anti-aliasing techniques Using Gaussian Filter.
Step 3: Obtain the dimensions (height and width) of the input cover image
Step 4: The cover image is resized to half its original resolution using a down sampling factor of 2 in both axes to get new size of the image is:

$$\frac{num\ rows}{2} \times \frac{num\ columns}{2}$$

Step 5: down sampled by a factor of 2 using anti-aliasing techniques to prevent aliasing effects and preserve image quality during resolution reduction.
Step 6: End

Step4: The real data is binarized (Bit plane slicing) and mapped into a format compatible with the secret sharing scheme for secure embedding into the alpha channel.
Secret sharing scheme.
Adi Shamir developed the cryptographic technique known as Secret Sharing, which aims to divide a secret into several independent parts to ensure its protection. This method relies on distributing the secret in such a way that it cannot be recovered unless a sufficient number of these parts are available. Assuming that S represents the secret to be protected, it is divided into N parts as follows:
S1, S2, S3,..., Sn.
After that, a threshold number K is determined, which represents the minimum number of parts required to reconstruct the secret, such that: If fewer than Kparts are available, it is impossible to recover the secret S; that is, it cannot be reconstructed using $K-1$ parts or fewer.[26]
process of obtaining the binarization will be done using Bit plane slicing [27], the bit plane slicing of the down sampled color image is performed. This image contains 24 bit- planes: 8 bit- planes for red, 8 bit- planes for green, and 8 bit- planes for blue. Algorithm.2 illustrates the process of obtaining the bit- planes for the three colors:

Algo.2: **Perform bitplane slicing on the Scaled-down image and Shamir secret sharing**

Input: Scaled-down image

Output: 15 Secret Bitplanes of Scaled-down image

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

Step 1: Scaled-down image selection process
Step 2: Get of the red, green and blue planes
Step 3: Doing bitplane slicing to R, G and B channels

$$RP_k = \left\{ R(i,j,k) \middle| \begin{matrix} 1 \le i \le r, 1 \le j \le c \\ R(i,j,k) \in \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \quad (3)$$

RP_1, RP_2, RP_3, RP_4, RP_5, RP_6, RP_7 *and* RP_8.

$$GP_k = \left\{ G(i,j,k) \middle| \begin{matrix} 1 \le i \le r, 1 \le j \le c \\ G(i,j,k) \in \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \quad (4)$$

GP_1, GP_2, GP_3, GP_4, GP_5, GP_6, GP_7 *and* GP_8.

$$BP_k = \left\{ B(i,j,k) \middle| \begin{matrix} 1 \le i \le r, 1 \le j \le c \\ B(i,j,k) \in \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \quad (5)$$

BP_1, BP_2, BP_3, BP_4, BP_5, BP_6, BP_7 *and* BP_8.

Step 4: We will take the five most important planes from each color plane (5 planes from Red: RP_4, RP_5, RP_6, RP_7 *and* RP_8, 5 planes from Green: GP_4, GP_5, GP_6, GP_7 *and* GP_8 and 5 planes form Blue: BP_4, BP_5, BP_6, BP_7 *and* BP_8), so we will have 15 planes that represent important data to complete the authentication and repair process.
Step 5: Generate n shares by evaluating the polynomial $Poly(i,j)$ distinct non zero points x1, x2.

$$Share_m(i,j) = Poly_{i,j}(x_m)$$

The data of bit-planes is shared and only five most important planes from each color bit-planes selected. Let it be SRP_4, SRP_5, SRP_6, SRP_7 *and* SRP_8 for Bitplanes Red. SGP_4, SGP_5, SGP_6, SGP_7 *and* SGP_8 for Bitplanes Green. SBP_4, SBP_5, SBP_6, SBP_7 *and* SBP_8 for Bitplanes Blue.
Step 6: End

Step 5: ***Mapping and Embedding***
This step is actually the most important step in our work. In this step, an alpha channel will be added to the input image, and it must be the same size. Then, the bit planes of the computed secret shares will be merged into the alpha channel, and the alpha channel will be merged with the cover image. After embedding the bit planes of the secret shares, we will obtain the alpha stego channel. Algorithm 3 and Figure 2 illustrates this entire process. The input to this algorithm will be the alpha channel and the bit planes of the secret shares for the red, green, and blue bit planes. The output of this algorithm is the alpha stego channel.

Algo.3: Mapping and Embedding Bitplanes secret shares in alpha channel

Input: Alpha Channel and Bitplanes secret shares of red, green and blue planes

Output: Stego Alpha Channel ($Stego_{alpha}$)

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

Step 1: Add the alpha channel, ensuring that its dimensions match those of the cover image
Step 2: Get SRP_4, SRP_5, SRP_6, SRP_7 *and* SRP_8 for Bitplanes Red. SGP_4, SGP_5, SGP_6, SGP_7 *and* SGP_8 for Bitplanes Green. SBP_4, SBP_5, SBP_6, SBP_7 *and* SBP_8 for Bitplanes Blue.
Step 3: The alpha channel is initialized as an array with a constant value of 255 as in the following equation:

$$A_k = \left\{ alpha(x,y,k) \middle| \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ alpha(x,y,k) \in \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \quad (6)$$

$A_1, A_2, A_3, A_4, A_5, A_6, A_7$ *and* A_8 . The binary values of these levels are all ones.
Step 4: We'll create new bit planes the size of the cover image. SRP_4 *and* SRP_5 will be horizontally connected, SRP_6 *and* SRP_7 will also be horizontally connected, and these two pairs will be vertically connected. Repeat the same process for the other bit levels as well. A comma is used for horizontal connection, and a semicolon is used for vertical connection.
BP1=[SRP_4 , SRP_5 ; SRP_6 , SRP_7]
BP2=[SRP_8 , SGP_4 ; SGP_5 , SGP_6]
BP3=[SGP_7 , SGP_8 ; SBP_4 , SBP_5]
BP4=[SBP_6 , SBP_7 ; SBP_8 , all ones with dimensions equal to the Scaled-down image size]
Step 5: Construct and form a stego alpha channel by multiplying the binary equivalent multiplier. As follows:

$$Stego_{alpha} = BP1 * 2^0 + BP2 * 2^1 + BP3 * 2^2 + BP4 * 2^3 + A_5 * 2^4 + A_6 * 2^5 + A_7 * 2^6 + A_8 * 2^7 \quad (7)$$

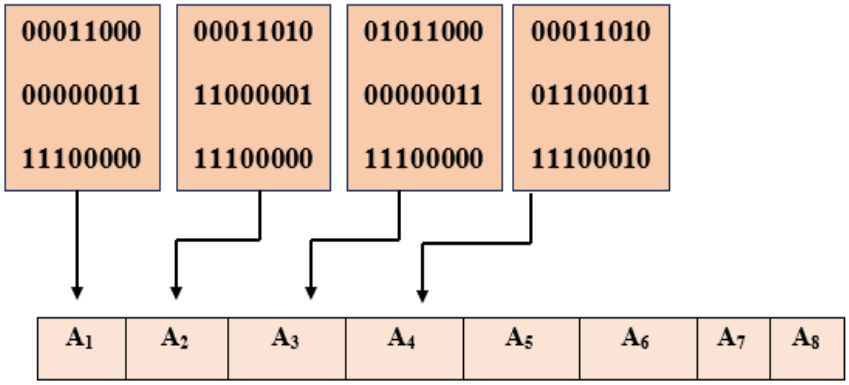


Figure 2 Embedding Bitplanes secret shares in alpha channel

Step 6: End

The final stage in the process of embedding secret data for authentication and repair is to create and generate a stego color image. The generated stego alpha channel is combined with the cover image to produce the final stego color image. Algorithm 4 illustrates this process. The algorithm's inputs are the stego alpha channel and the cover image, and the output is the stego color image.

Algo.4: create and generate a stego color image

Input: stego alpha channel and the cover image

Output: stego color image (SCI)

Step 1: Get Stego alpha channel and Cover Image
Step 2: Combine cover image and stego alpha channel together to produce the stego color image: Stego color Image: SCI= Cover Image + Stego Alpha Channel
Step 3: End

3.2 Stego Color Image Authentication and Verification

This process involves verifying the input Stego image and its self- repairing capability. First, the secret authentication data is extracted from the Stego image. In parallel, new authentication data is

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

computed from the Stego image. The secret authentication data is then compared with the calculated authentication data. If they match, the image is considered authentic. If they do not match, the image is considered inauthentic, and steps are taken to identify the tampering and self- repair the image. The Figure 3 illustrates this process:

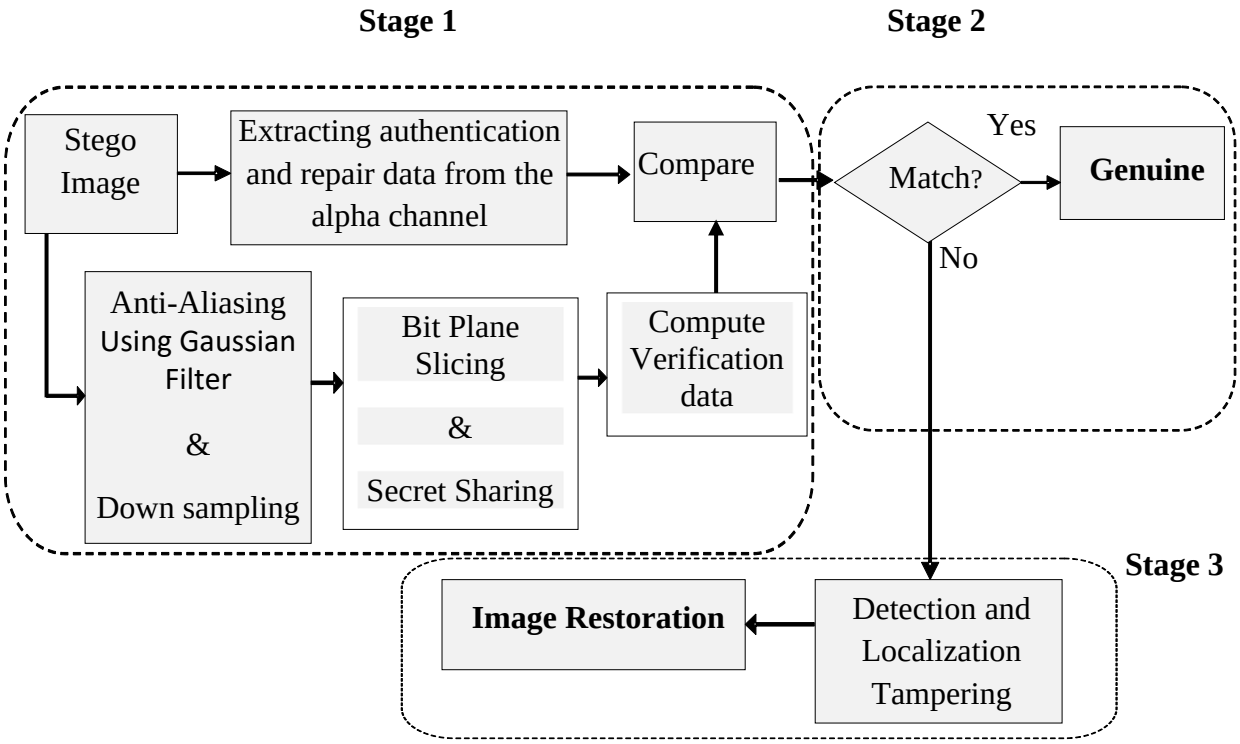


Figure 3 authentication process that involves verifications and self-repairing a color PNG image

As shown in the Figure 3, the Stego image authentication process involves three important stages. Stage 1 about Extraction of secret authentication data from alpha channel [28]. Stage 2 is about Verification of the stego image. Stage 3 is about self-repairing of original image

Stage 1: Extraction of secret authentication data from alpha channel
Stage 2: Verification of the stego image if authentic or not authentic
Stage 3: process to self-repairing of original image

The above three steps will be discussed and explained in Algorithm 5. In Algorithm 5, the stego color image SCI is the input, and the output is the recovered image (self-repairing) RI.

Algo.5: *Authentication and Verification* of *Stego color Image*

Input: *stego color image SCI*

Output: self-*recovered image RI*

Stage 1: Extraction of secret authentication data from alpha channel
Step 1: Get *stego color image SCI*
Step 2: Extract alpha channel from stego color PNG image
Step 3: We take the first four Bitplanes of the alpha channel using bit-plane slicing. Let's call them SA_1, SA_2, SA_3, and SA_4.
Step 4: Bit level SA_1 will be divided into four parts. Since SA_1 is a sequence of SRP_4, SRP_5, SRP_6, *and* SRP_7. SA_2 is further divided into four parts SRP_8, SGP_4, SGP_5 and SGP_6 and SA_3 is further divided into four parts SGP_7, SGP_8, SBP_4 and SBP_5 and finally SA_4 is further divided into four

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

parts SBP_6, SBP_7, SBP_8 and all ones with dimensions equal to the Scaled-down image size.

Step 5: In this step, we will combine the data extracted from the alpha channel to form authentication data for matching and repair. Let's call it A_{Data}.

red data = $SRP_4 * 2^3 + SRP_5 * 2^4 + SRP_6 * 2^5 + SRP_7 * 2^6 + SRP_8 * 2^7$

green data = $SGP_4 * 2^3 + SGP_5 * 2^4 + SGP_6 * 2^5 + SGP_7 * 2^6 + SGP_8 * 2^7$

blue data = $SBP_4 * 2^3 + SBP_5 * 2^4 + SBP_6 * 2^5 + SBP_7 * 2^6 + SBP_8 * 2^7$

A_{Data}= Concatenate (red data, green data, blue data)

Step 6: In this step, bit-plane slicing will be performed on the color compone (8) G, B) of the resulting color image after the down sampling process. We will then take the five most significant planes from each color component to begin calculating the verification data. These levels are as follows:

RL_4, RL_5, RL_6, RL_7 and RL_8.
GL_4, GL_5, GL_6, GL_7 and GL_8.
BL_4, BL_5, BL_6, BL_7 and BL_8.

Step 7: Generate n shares by evaluating the polynomial $Poly(i,j)$ distinct non zero points x1, x2.

$$Share_m(i,j) = Poly_{i,j}(x_m)$$

The data of bit-planes is shared and only five most important planes from each color bit-planes selected. Let it be VRL_4, VRL_5, VRL_6, VRL_7 and VRL_8 for Bitplanes Red. VGL_4, VGL_5, VGL_6, VGL_7 and VGL_8 for Bitplanes Green. VBL_4, VBL_5, VBL_6, VBL_7 and VBL_8 for Bitplanes Blue.

Step 8: We will now calculate the secret bit planes that resulted in the previous step and then combine them to obtain the verification data to perform the matching process with the original secret data:

V_red data = $VRL_4 * 2^3 + VRL_5 * 2^4 + VRL_6 * 2^5 + VRL_7 * 2^6 + VRL_8 * 2^7$

V_green data = $VGL_4 * 2^3 + VGL_5 * 2^4 + VGL_6 * 2^5 + VGL_7 * 2^6 + VGL_8 * 2^7$

V_blue data = $VBL_4 * 2^3 + VBL_5 * 2^4 + VBL_6 * 2^5 + VBL_7 * 2^6 + VBL_8 * 2^7$

V_{Data}= Concatenate (V_red data, V_green data, V_blue data)

Stage 2: Verification of the stego color image (9)

Step 9: If ($A_{Data} = V_{Data}$)

{
The image is genuine,
}
Else
{
Authentication failed — image restoration is needed,
}

Stage 3: process to self-repairing of original image

Step 10: Here in this step the data repair process will be done

If (A_{Data} ~ = VData)
{
RI (i, j) = A_{Data} (i, j)
}

Step 11: RI is upscaled by a factor of 2

Step 12: The final output RI is treated as the self-repaired version of the image.

Step 13: End

4. Results and Discussion

In this paragraph, we show simulation results to evaluate the performance of the purpose algorithm for authenticating color scanned images and documents. The primary goal of this algorithm is to determine whether the scanned image or document is authentic. If authentication fails, the algorithm aims to identify the tampered region and recover the tampered data. The proposed algorithm focuses on achieving the following objectives: embedding the secret authentication data directly within the host file instead of a separate file; maintaining high visual quality of the image after embedding the authentication data; detecting and identifying tampered regions in the image; restoring the original content of the tampered regions; and achieving security and robustness against attackers.

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

After applying the developed algorithm, the quality of both the stego image (the image containing the secret data) and the repaired image must be evaluated. Various objective quality metrics were used to assess quality. Image quality assessment (IQA) [29-30-31] methods are classified into two types: full reference (FR) and non-reference (NR). In this study, full-reference IQA metrics were used to analyse the algorithms' performance. 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).
Experiments will be conducted on color images and color scanned documents. There are no image dimensions restrictions, as the images will be of larger dimensions than the traditional image sizes used in reference and research.
The results will be displayed in the following sequence for clarity:

1. Embedded the secret data (authentication and repair data) in the alpha channel
2. Calculating quality parameters in the Embed process and displaying values
3. Applying different types of attacks on color images
4. Perform color image repairing, display, and calculate quality parameters.

4.1 Embed authentication data

A real-world scanned color document image was chosen, specifically an image of Aadhaar Color document Image It is a scanned color image. as the cover image for the test application. because most authentication techniques focus only on color images without emphasizing scanned document images. The size of this color document image is 1112 x 700. An alpha channel will be added to this cover image, and then the authentication and repair data will be embedded in the alpha channel as Figure 4 follows:

(a)

(b)

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

(c)

Figure 4 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
Alpha Channel MSE	24.628
Alpha Channel SC	0.978781
Alpha Channel AD	2.75375
Alpha Channel NCC	0.999866
Alpha Channel EC	6227200
Alpha Channel NBE	3113600

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

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

i. Cropping Images
ii. Text-based assault
iii. Salt & Pepper noise
iv. Gaussian noise
v. Enhancement

Now algorithm 5 is used for all above attacks for authenticity verification and data recovery.

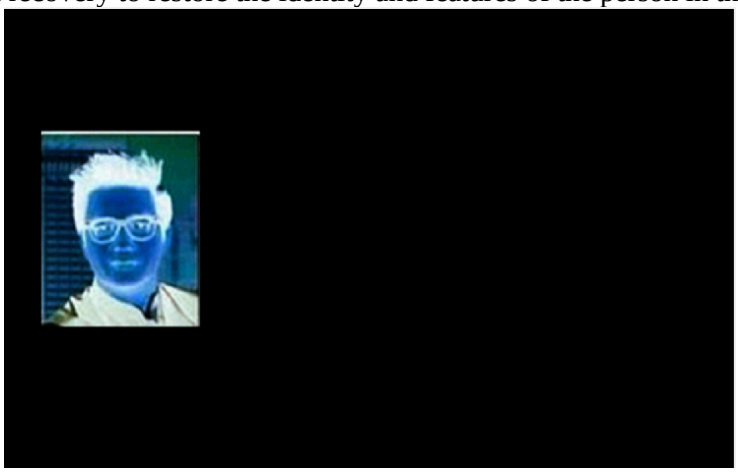
i. Cropping Images Attack, Authenticity verification and data recovery

The face of the person in the color image will be cropped to hide landmarks and identity. Figure 5 shows the cropped image:

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

Figure 5 Cropping attack on color Image

The Stego image has been cropped to hide features and identity. The cropped image will now be verified and its data recovery to restore the identity and features of the person in the image.



(a)

(b)

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

(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. Figure 6 (a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 6(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

Image Parameter (Quality) Color document Image	Values
PSNR (dB)	44.7253
MSE	2.05738
NCC	0.997663
SC	0.99839
AD	0.247698
SSIM	0.998984

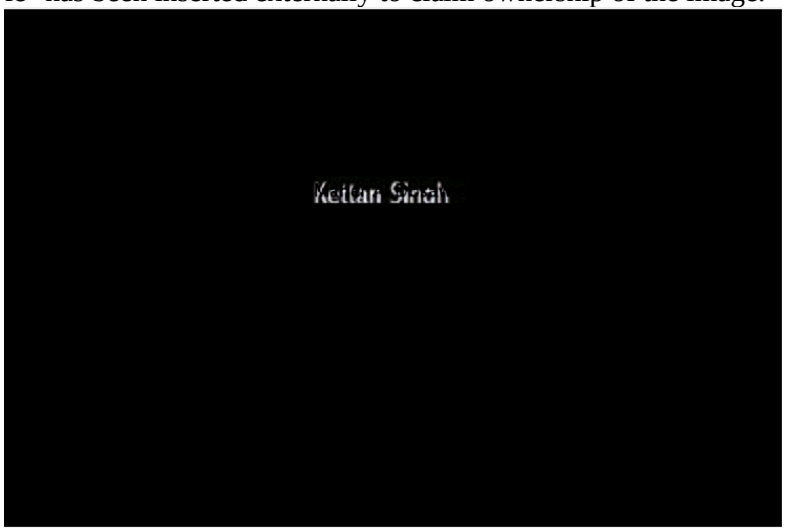
ii. Text-based assault, Authenticity verification and data recovery

An attack that adds external text to an image is very dangerous because it changes the ownership of the image document. Figure 7 illustrates a text-on-image attack:

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

Figure 7 Text attack on color Image

Anyone can claim ownership of an image by inserting the required text. In Figure 7 above, the text "Maher Al Dbsawie" has been inserted externally to claim ownership of the image.



(a)

(b)

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

(c)

Figure 8. Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 8 shows the detailed results of the authentication and data recovery. Figure 8(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 8(b) shows the identification of the tampered region, and Figure 8(c) is the repaired image. This image is obtained by matching the authentication data with the tampered area.

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 attack

Image Parameter (Quality) Color document Image	Values
PSNR (dB)	49.0199
MSE	0.797343
NCC	0.999992
SC	0.999716
AD	0.0290802
SSIM	0.999417

iii. Salt & Pepper noise, Authenticity verification and data recovery

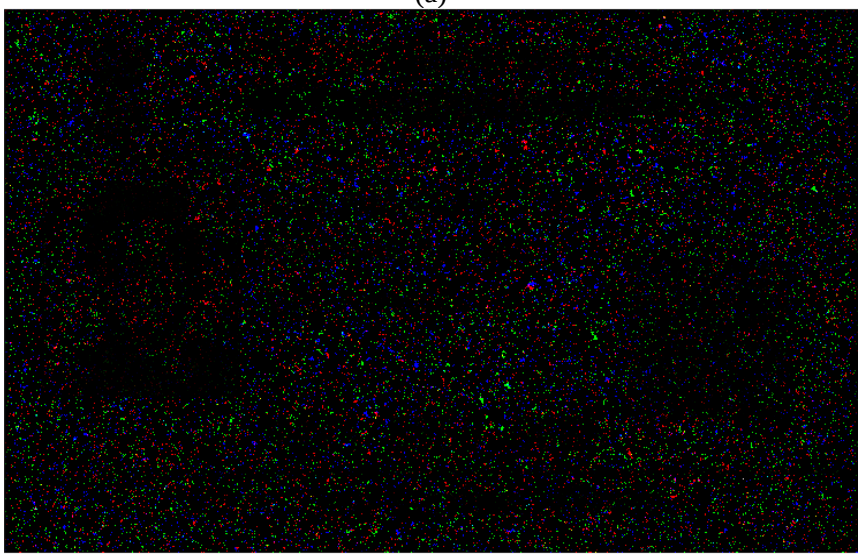
This type of attack is considered an unintended attack and can result from a problem in the transmission network. Figure 9 illustrates a salt-and-pepper noise attack on a color image:

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

Figure 9 Salt & Pepper noise attack on color Image

Here the noise of salt and pepper has been added with a density of its value 0.2. This means that 20% of all image pixels will be affected, which is a very noticeable effect.

(a)



(b)

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

(c)

Figure 10 Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 10 shows the detailed results of the authentication and data recovery. Figure 10(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 10(b) shows the identification of the tampered area, and Figure 10(c) is the repaired image. This image is obtained by matching the authentication data with the tampered area. 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 Salt & Pepper noise attack

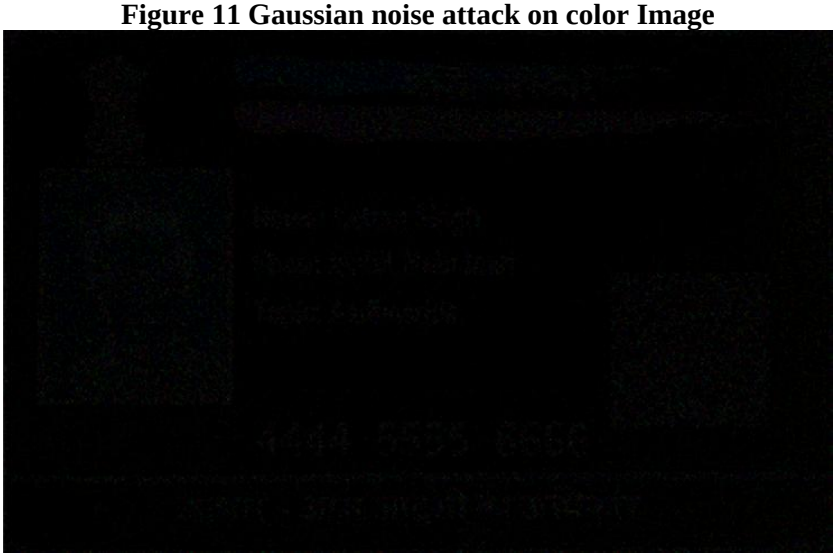
Image Parameter (Quality) Color document Image	Values
PSNR (dB)	32.1914
MSE	35.1007
NCC	0.999741
SC	0.972163
AD	3.09844
SSIM	0.949609

iv. Gaussian noise Attack, Authenticity verification and data recovery

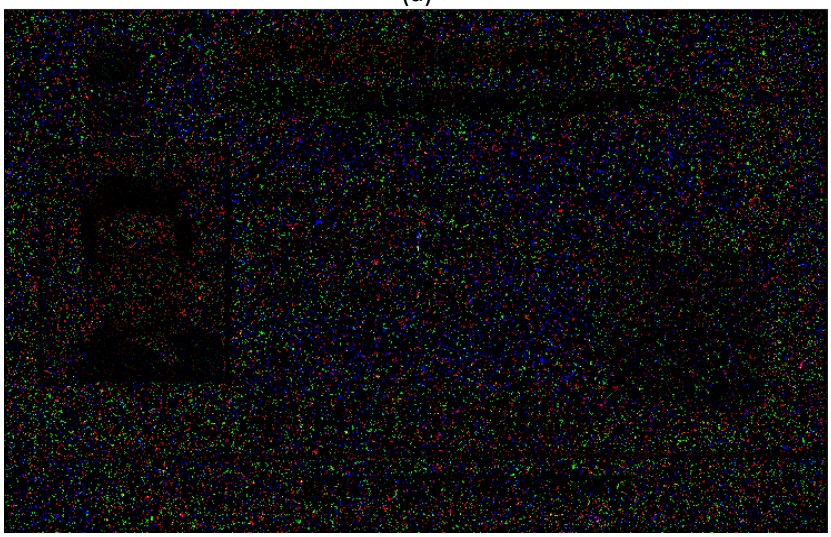
This type of attack is considered unintentional and occurs naturally as a result of errors or random fluctuations in the system. It adds a soft, hazy, or cloudy effect. Figure 11 illustrates a Gaussian noise attack on a color image:

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

Figure 11 Gaussian noise attack on color Image



(a)



(b)

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

(c)

Figure 12. Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 12 shows the detailed results of the authentication and data recovery. Figure 12(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 12(b) shows the identification of the tampered area, and Figure 12(c) is the repaired image. This image is obtained by matching the authentication data with the tampered area.

The quality parameters of the repaired and restored color image were calculated and are shown in Table 6:

Table 6 quality parameters for color Image for Gaussian noise attack

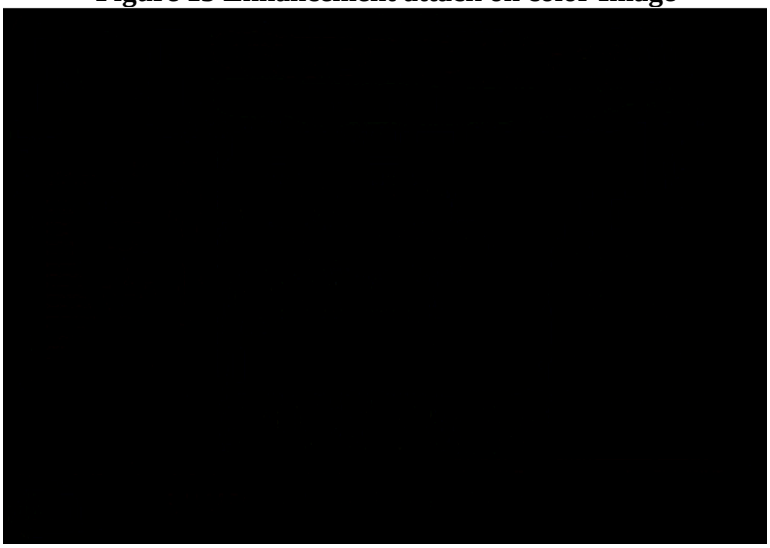
Image Parameter (Quality) Color document Image	Values
PSNR (dB)	31.6044
MSE	41.2029
NCC	0.999676
SC	0.973039
AD	3.01451
SSIM	0.918003

v. Enhancement Attack, Authenticity verification and data recovery

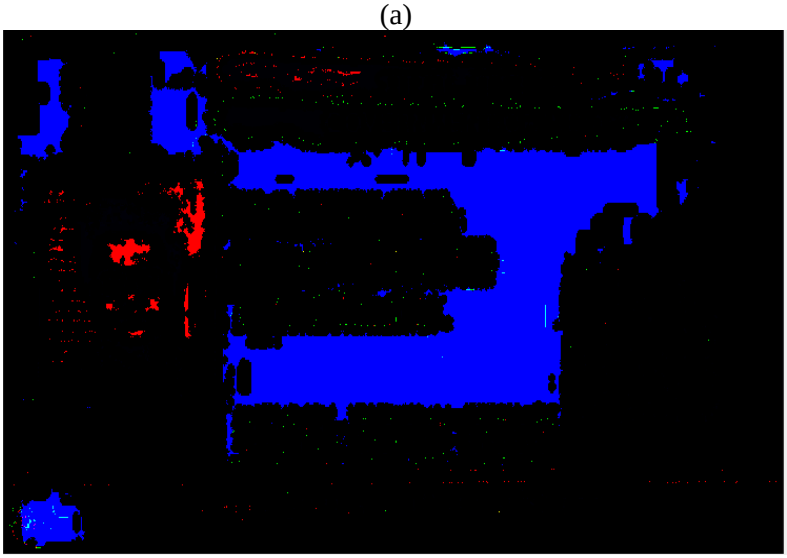
It is a type of attack that aims to uncover or enhance confidential or hidden information in images or digital media by improving image quality or magnifying hidden details. This type of attack is considered intentional. Some enhancement techniques may stimulate or amplify existing noise. Figure 13 illustrates an enhancement attack on a color image:

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

Figure 13 Enhancement attack on color Image



(a)



(b)

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

(c)

Figure 14 Authentication, verification and Data recovery of color Image (a) Subtraction of Authentication data and verification data (b) Tampered area identification (c) Repaired Image

Figure 14 shows the detailed results of the authentication and data recovery. Figure 14(a) shows the subtraction of the authentication data embedded in the alpha channel and the extracted data for color image verification. Figure 14(b) shows the identification of the tampered area, and Figure 14(c) is the repaired image. This image is obtained by matching the authentication data with the tampered area.

The quality parameters of the repaired and restored color image were calculated and are shown in Table 7:

Table 7 quality parameters for color Image for Enhancement noise attack

Image Parameter (Quality) Color document Image	Values
PSNR (dB)	32.8904
MSE	32.1718
NCC	0.999777
SC	0.971467
AD	3.16642
SSIM	0.964166

4.3. Comparison

The proposed methodology in this research is compared with previous methodologies and literature from different authors in the same category of color image authentication and repairability, and the comparison is shown in the following Table 8:

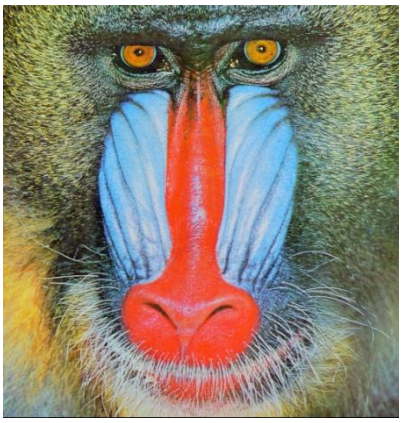
Table 8 Comparison of proposed methods

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

N	Ref	Image size used	Alteration in stego image	For color image and color document image	Security Robustness	Ability to repair data	Attack Coverage	Authentication Granularity
1	Lee, Che-Wei, and Wen-Hsiang Tsai (2013).[19]	512x512	No	No. For color image	High (limited evaluation scope)	No	Content tampering attacks	Pixel level
2	Sinhal, Rishi, Irshad Ahmad Ansari, and Chang Wook Ahn (2020).[20]	512x512	Yes	No. For color image	High (Tamper threshold <80%)	Yes If Tamper Rate <80 %	Content tampering and quality degradation	Block level
3	Nichal, Arjun, and Bhalachn (2021).[21]	512x512	No	No. For color image	Low	Yes	Content tampering and quality degradation	Pixel level
4	Che-Wei Lee (2024). [22]	512x512	No	No. For color image	High (Tamper threshold <60%)	Yes If Tamper Rate <60 %	Content tampering attacks	Block level
5	Molina-Garcia, Javier, [23] (2020)	512x512	Yes	No. For color image	High (Tamper threshold <80%)	Yes (If Tamper Rate <80%)	Content tampering and quality degradation	Block level
5	**Proposed Method**	**1112x700**	**No**	**Yes**	**High (extensive evaluation scope)**	**Yes**	**Content tampering and image quality attacks**	**Pixel level**

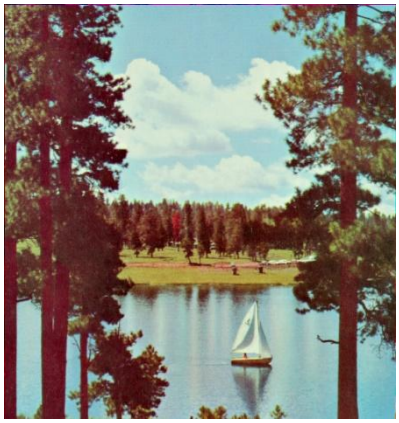
The average quality metrics of the recovered image, namely PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Measure), were compared with those of state-of-the-art methods in the field of color image authentication. The comparison considered the tampering rate (%) in the color image under various attack scenarios, including cropping attacks, Superimposing attacks, and several random tampering attacks. The test images (USC-SIPI Image Database color image) are shown in Figure 15, and the results are presented in Table 9.

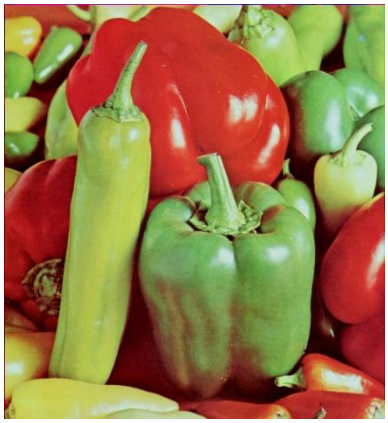
 ISSN:2302-8149
e-ISSN:2540-9719


Baboon 512x512


Lena 512x512

Airplane 512x512


Sailboat 512x512


Pepper 512x512

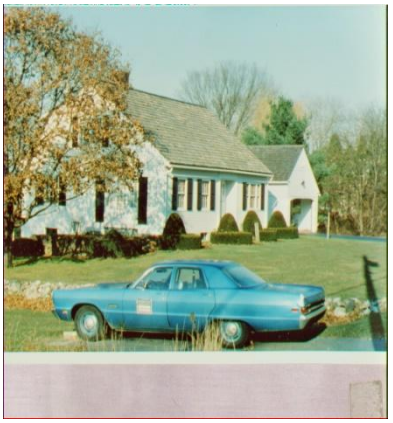

House 512x512

Figure 15 Test images

Table 9 Comparison of the average quality metric values between previous methods and the proposed method

Tampering Rate (%)	PSNR				SSIM			
	Molina-Garcia [23]	Sinhal, Rishi [20]	Che-Wei Lee [22]	**Proposed Method**	Molina-Garcia [23]	Sinhal, Rishi [20]	Che-Wei Lee [22]	**Proposed Method**
10	37.34	36.18	34.18	**43.79**	0.9714	0.9878	NA	**0.9991**
20	33.98	32.38	32.79	**39.83**	0.9390	0.9768	NA	**0.9977**
30	31.28	29.98	31.46	**37.67**	0.8977	0.9638	NA	**0.9950**
40	28.47	28.34	30.40	**36.45**	0.8368	0.9504	NA	**0.9929**
50	26.00	27.02	29.01	**35.57**	0.7571	0.9358	NA	**0.9904**
60	23.51	25.46	27.66	**34.84**	0.6460	0.9128	NA	**0.9869**
70	21.23	23.94	26.23	**34.22**	0.5157	0.8843	NA	**0.9835**
80	19.20	22.47	25.01	**33.72**	0.3958	0.8528	NA	**0.9805**
90	NA	NA	NA	**33.26**	NA	NA	NA	**0.9775**

Note: The values not calculated in some previous studies are indicated as not available (NA).

I conducted a comparison between my proposed methodology and the methodology presented in reference [22] as follows:
In the methodology [22], it is the latest methodology published to date in the field of color image authentication and recovery. the researcher relied on an effective and efficient method for authenticating color images and the possibility of restoring them. However, his methodology showed weakness in the self-repair process when the rate of destruction and tampering is greater than or equal to 60% of the image. The researcher relied on a Superimposing Attack using a white rectangle, which leads to image distortion and visual deception, as shown in Figure 16, which illustrates the

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

superimposing attack on an Airplane image of size 512x512 pixels, where the destruction rate appears to be greater than 60%.

(a)

(b)

Figure 16 Shows the attack process, (a) Airplane image, (b) attack on the Airplane image

In methodology [22]. The result of the data repair will be as shown in the Figure 17:

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

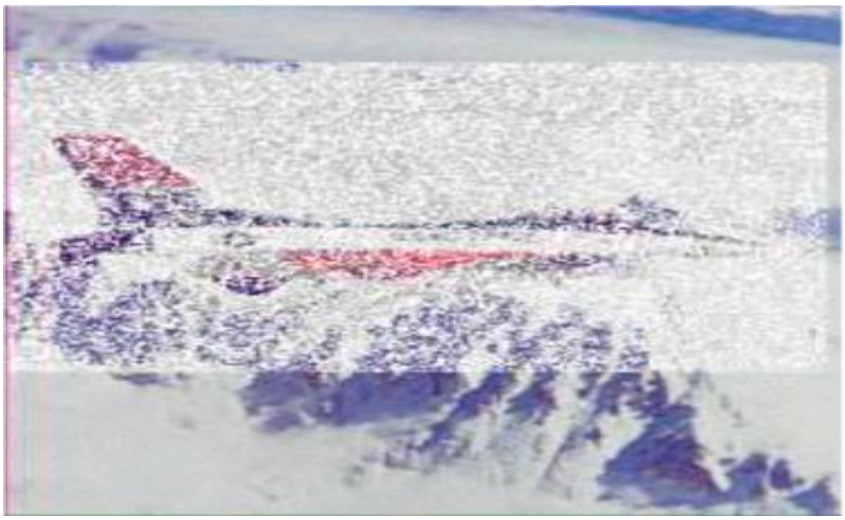


Figure 17 Result of the data repair process in methodology [22]

In Proposed Methods. The result of the data repair will be as shown in the Figure 18:

Figure 18 Result of the data repair process in Proposed Methods

The quality parameters of the repaired and restored color Airplane image were calculated and are shown in Table 10:

Table 10 quality parameters for color Airplane image

Image Parameter (Quality) Color Airplane Image	Values
PSNR (dB)	31.8592
MSE	29.651
NCC	0.999631
SC	0.975246
AD	2.23085

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

Image Parameter (Quality) Color Airplane Image	Values
SSIM	0.955981

5. Conclusion

The proposed system provides a robust and effective methodology for authenticating color scanned images and documents, utilizing the most significant data in each color channel (Red, Green, Blue). This data is determined using a bit-plane slicing technique for each channel separately, with the top five (Most Significant Bitplanes – MSBs) being used due to their high sensitivity to modifications. After extracting these significant levels, Shamir's Secret Sharing technique is applied to generate secret shares that are later used for authentication and repair. These shares are stored in the alpha channel added to the color image, providing an additional layer of protection. This will not affect the quality of the color image, as the authentication data will be embedded in a separate channel, which is the alpha channel.

Most techniques presented in the literature and research rely on embedding limited binary data within the image, such as digital signatures or identification codes, to verify the authenticity of the data and detect potential tampering. If verification is successful, this data can sometimes only be recovered, with the possibility of subsequent repair, without providing an effective mechanism for repairing the image content itself in the event of damage or modification. These data are used solely for authentication purposes.

The results demonstrated that the system is capable of detecting both minor and major alterations with high accuracy and provides an effective repair mechanism, even under attacks targeting image quality or content. These results confirm the system's effectiveness in achieving reliable authentication and accurate restoration in a variety of real-world scenarios. More than 90 percent of a tampered image can be recovered. Other advanced methodologies for video authentication and data repair against attacks such as rotation, compression, and other engineering attacks could be studied in the future.

- All the above results were obtained using MATLAB 2015a software to perform the calculations on a personal computer. Detailed specifications of the computer used are provided in Appendix 1.

Appendix 1

This appendix provides detailed specifications of the personal computer used to obtain the simulation results using MATLAB 2015a software:

CPU	Intel(R) Core (TM) i5-7200U CPU @ 2.50GHz 2.71
RAM	DDR4- 8 GB
GPU	Integrated (Intel HD Graphics 620)
ID_LAP	7B075AE7-682B-4B19-846B-4686961F7123
OS	Windows 10 Pro
Hard Disk	SSD-256GB

References

[1] Chen, Brian, and Gregory W. Wornell. "*Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding*." *IEEE Transactions on Information theory* 47.4 (2001): 1423-1443. https://doi.org/10.1109/18.923725

[2] Kundur, Deepa, and Dimitrios Hatzinakos. "*Digital Watermarking for Telltale Tamper Proofing and Authentication*." *Proceedings of the IEEE* 87.7 (1999): 1167-1180. https://doi.org/10.1109/5.771070

[3] Bonafè, Barbara, et al. "*Alpha Channel Fragile Watermarking for Color Image Integrity Protection*." *Journal of Imaging* 3.4 (2017): 53. https://doi.org/10.3390/jimaging3040053

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

[4] T. T. K. Hue, N. T. Linh, M. Nguyen-Duc and T. M. Hoang, "*Data Hiding in Bit-Plane Medical Image using Chaos-based Steganography*," 2021 International Conference on Multimedia Analysis and Pattern Recognition (MAPR), Hanoi, Vietnam, 2021, pp. 1-6, DOI: 10.1109/MAPR53640.2021.9585243.

[5] Lei, Joanna Tan Lei, Liew Siau Chuin, and Ferda Ernawan. "*An Image Watermarking based on Multi-Level Authentication for Quick Response Code*." 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM). IEEE, 2021. https://doi.org/10.1109/ICSECS52883.2021.00082

[6] Lian, Kiung Siew, Liew Siau Chuin, and Ferda Ernawan. "*Reversible Face Watermarking Scheme using Hash Function for Tamper Localization and Recovery.*" 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM). IEEE, 2021. https://doi.org/10.1109/ICSECS52883.2021.00018

[7] X. Yuan and Q. Zhang, "*Halftoning-based Fragile Watermarking Approach for Digital Image Self Recovery*," 2022 7th International Conference on Signal and Image Processing (ICSIP), Suzhou, China,2022, pp. 352-355, DOI: 10.1109/ICSIP55141.2022.9886130.

[8] 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. https://doi.org/10.1109/ICOCO53166.2021.9673559

[9] Shamir, Adi. "*How to Share a Secret*." *Communications of the ACM* 22.11 (1979): 612-613.

[10] Linda, Mary, et al. "*Ramp Secret Sharing Approach to Authentication and Data Repairing for Document Image*." International Journal of Engineering Research and Applications 4.4 (2014): 81-86.

[11] Wu, Min, and Bede Liu. "*Data Hiding in Binary Image for Authentication and Annotation*." IEEE Transactions on Multimedia 6.4 (2004): 528-538. https://doi.org/10.1109/TMM.2004.830814

[12] Yang, Huijuan, and Alex C. Kot. "*Binary Image Authentication with Tampering Localization by Embedding Cryptographic Signature and Block Identifier*." IEEE Signal Processing Letters 13.12 (2006): 741-744. https://doi.org/10.1109/LSP.2006.879829

[13] Tzeng, Chih-Hsuan, and Wen-Hsiang Tsai. "*A New Approach to Authentication of Binary Images for Multimedia Communication with Distortion Reduction and Security Enhancement*." IEEE Communications Letters 7.9 (2003): 443-445. https://doi.org/10.1109/LCOMM.2003.815656

[14] Arya, K. V., and Akanksha Bandil. "*An Improved Image Authentication Technique using Random-Sequence based Secret-Sharing Scheme*." 2014 9th International Conference on Industrial and Information Systems (ICIIS). IEEE, 2014. https://doi.org/10.1109/ICIINFS.2014.7036660

[15] Lee, Che-Wei, and Wen-Hsiang Tsai. "*Authentication of Binary Document Images in PNG Format based on a Secret Sharing Technique.*" 2010 International Conference on System Science and Engineering. IEEE, 2010. https://doi.org/10.1109/ICSSE.2010.5551726

[16] Nichal, Arjun, and Bhalchandra Godbole. "*Grayscale Image Authentication with Data Repair Capability*." *2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. IEEE, 2021. https://doi.org/10.1109/SMARTGENCON51891.2021.9645794

[17] 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

[18] 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

[19] 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. https://doi.org/10.1016/j.sigpro.2013.01.009

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

[20] 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. https://doi.org/10.1109/ACCESS.2020.3035428

[21] Nichal, Arjun, and Bhalachnadra Godbole. "*Color Image Authentication with Data Repair Capability*." International Journal of Electrical Engineering and Technology (IJEET).2021. https://doi.org/10.34218/IJEET.12.6.2021.0042

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

[23] Molina-Garcia, Javier, et al. "*An Effective Fragile Watermarking Scheme for Color Image Tampering Detection and Self-Recovery*." *Signal Processing: Image Communication* 81 (2020): 115725. https://doi.org/10.1016/j.image.2019.115725

[24] Yang, Huijuan, and Alex C. Kot. "*Pattern-based Data Hiding for Binary Image Authentication by Connectivity-Preserving*." *IEEE Transactions on Multimedia* 9.3 (2007): 475-486. https://doi.org/10.1109/TMM.2006.887990

[25] Rafeal Gonzalez et al., "*Digital Image Processing*", 3rd edition, published by Pearson Education, Inc, 2008.

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

[27] Karthika, M., and Ajay James. "*A Novel Approach for Document Image Binarization using Bit-Plane Slicing*." *Procedia Technology* 19 (2015): 758-765. https://doi.org/10.1016/j.protcy.2015.02.107

[28] Che-Wei Lee et al, "*A Secret-Sharing-based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability*", IEEE Transactions on Image Processing, Vol. 21, No. 1, pp 207-218, January 2012. https://doi.org/10.1109/TIP.2011.2159984

[29] 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.

[30] 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

[31] 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