Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Advanced Authentication And Recovery In Grayscale Imaging Via Alpha Layer And Secret Sharing

Maher AL Dbsawie[1] , Prof .Soliman Alasli[2] , Hassan AL Jabbouli[3]

[1]University of Idlib, Faculty of Informatics Engineering, Department of Software Engineering
Idlib, Idlib, Syria maher.dbsawie@idlib-university.com
[2]University of Idlib, Faculty of Electrical Engineering, Department of Digital communications
Idlib, Idlib, Syria
alasli.soliman@gmail.com
[3]Associate Professor. University of New York , Courant Institute of Mathematical Sciences New York, New York, USA ha2285@nyu.edu

Maintaining the authenticity and integrity of grayscale images is crucial in the field of digital imaging, particularly in situations when image data is essential. This study provides an advanced framework that uses secret sharing techniques and the synergistic properties of alpha layers for grayscale image authentication and recovery. To improve security without changing the original picture data, the suggested approach embeds authentication information in the alpha layer, a channel that is generally ignored in grayscale images. By dividing the authentication data into several shares and integrating secret sharing, this method is further strengthened and only authorized parties are able to reconstruct and validate the picture. In addition to verifying the image, this two-pronged approach offers strong data recovery capabilities, enabling the restoration of damaged or deleted areas. The outcomes of the experiments show how well this strategy works to preserve picture quality while offering excellent security and dependability for image authentication and restoration. The suggested method significantly improves the security of grayscale photos, which makes it ideal for applications that need high standards of secrecy and data integrity.

Keywords: Authentication, Data Hiding, Tamper Detection, Watermarking, secrete sharing, Alpha layer.

Introduction

The old proverb that goes, "The photograph doesn't lie," is no longer accurate because of the accessibility of strong image editing tools. Because digital images are so simple to work with, develop, and store, they have become increasingly popular. Subjectively, determining which photographs are altered and which are authentic is very difficult. The credibility that

photography has attained has diminished due to technological advancements. picture authentication methods guard against malicious picture tampering during the whole transmission and storage process. A trustworthy image authentication system must safeguard an image from the moment it is created until it is used in its final form. A digital image is a way to store significant data. Nonetheless, the rapid advancement of digital technology has made it simple to alter digital picture contents in a way that is invisible to the human eye. Thus, the problem is to guarantee the validity and integrity of a digital image. Particularly for images of documents whose security needs to be preserved, efficient answers to this kind of picture authentication problem should be devised [1]–[2]. Should it prove that some of a document image has been illegally altered, erased content is also expected to be restored. Such image content authentication and self-repair capabilities are helpful for the security protection of digital documents in many fields, including critical certificates, signed digital images, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, final wills and testaments and so forth [3]. Generally speaking, authenticity is a relative concept; an object's authenticity is dependent upon a genuine source or certain type of representation. Authentication usually entails confirming that the connections and rules that should be present in an authentic copy of the test material are still there. Generally speaking, authenticity is a relative concept; the genuineness of an object depends on a reference or a certain kind of portrayal approved as legitimate. A frequent approach of attaining authenticity is to find out if particular connections and rules expected to exist in an authentic copy still exist in the test material. Figure 1 shows a watermark based picture authentication method. The cover picture[4] helps to apply the watermark. Following watermark extraction, at the receiving end we can determine whether the image has been changed.

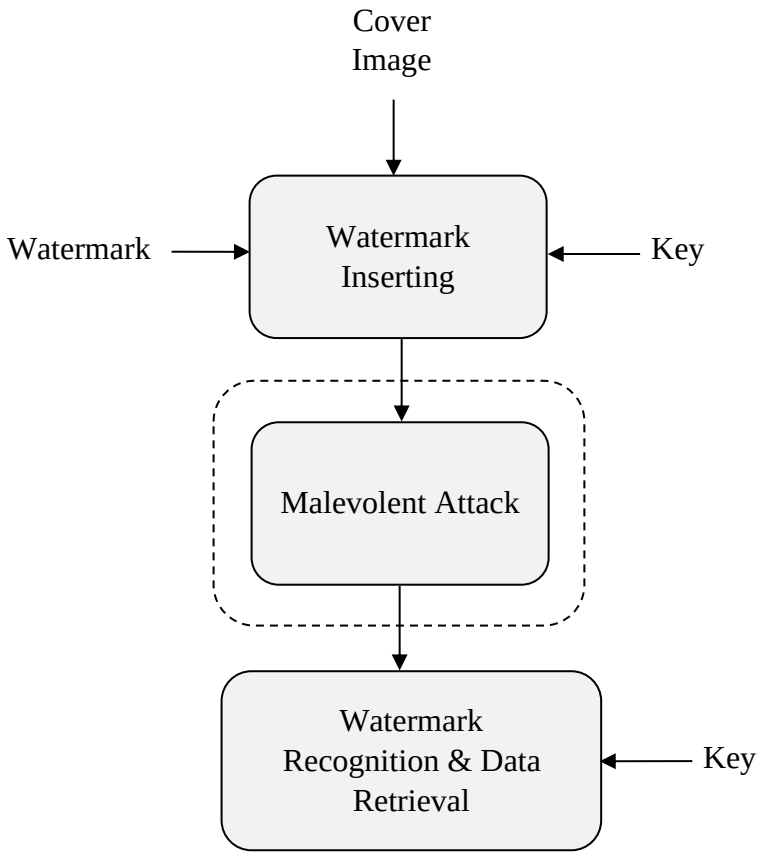


Figure 1 Simple image authentication scheme based on watermarks

Three essential components define digital watermarking algorithms: watermark embedding techniques, watermark extraction methods, and watermark detection systems. Figure 1 shows the actions of a generic watermark system. An algorithm gathers the data to be embedded and the host throughout the embedding process generates a watermarked image. After that, the watermarked picture is either sent or saved. Alteration of digital content is seen as attack on it. A "watermark attack" is a sort of digital data attack whereby the assailant may identify a specifically produced piece of data even in the lack of the encryption key[5]-[6]. The kind of assaults should be given special attention since they might improve watermarking methods and create more appropriate benchmarks.
The efficacy of any watermarking technique has to be investigated. Seven factors need to be considered when evaluating an image authentication technique [7]-[8].

Sensitivity: Any alterations or modifications to the content must be detectable by the authentication system. Strict authentication systems need the detection of any alteration, not only content modification.

Robustness: Another synonym for robustness is tolerance. The authentication mechanism must be able to withstand changes made for content preservation. This feature is only applicable to algorithms that provide a selective authentication service.

Localization: The modified image regions must be recognized by the authentication system.

Recovery: Partially or completely changed picture regions must be reconstructed by the authentication system.
Security: Any attempt to fabricate the authentication data must be thwarted by the authentication system.

Portability: The authentication system needs to be able to move the signature together with the protected picture throughout any kind of processing, storing, or transmission.

Complexity: Real-time techniques that are neither laborious nor slow must be used by the authentication system.

Methodology
A digital image is a way to store significant data. Nonetheless, the rapid advancement of digital technology has made it simple to alter digital picture contents in a way that is invisible to the human eye. Thus, the problem is to guarantee the validity and integrity of a digital image. Developing efficient techniques to address this type of picture authentication issue is preferable, especially when dealing with photos of documents whose confidentiality needs to be maintained. It is also envisaged that deleted material can be restored in the event that it is confirmed that a portion of a document image has been unlawfully changed. Such image content authentication and self-repair capabilities would help with security protection of digital documents in many spheres, including critical certifications, signed papers, scanned checks, circuit diagrams, art drawings, design drafts, final wills and testaments, and so forth [9].

I. Creation of the Stego Image
The primary step is the creation of the stego image. The carrier is embedded with the data needed for authentication throughout this operation. The steps involved in integrating real data are detailed in Figure 2.

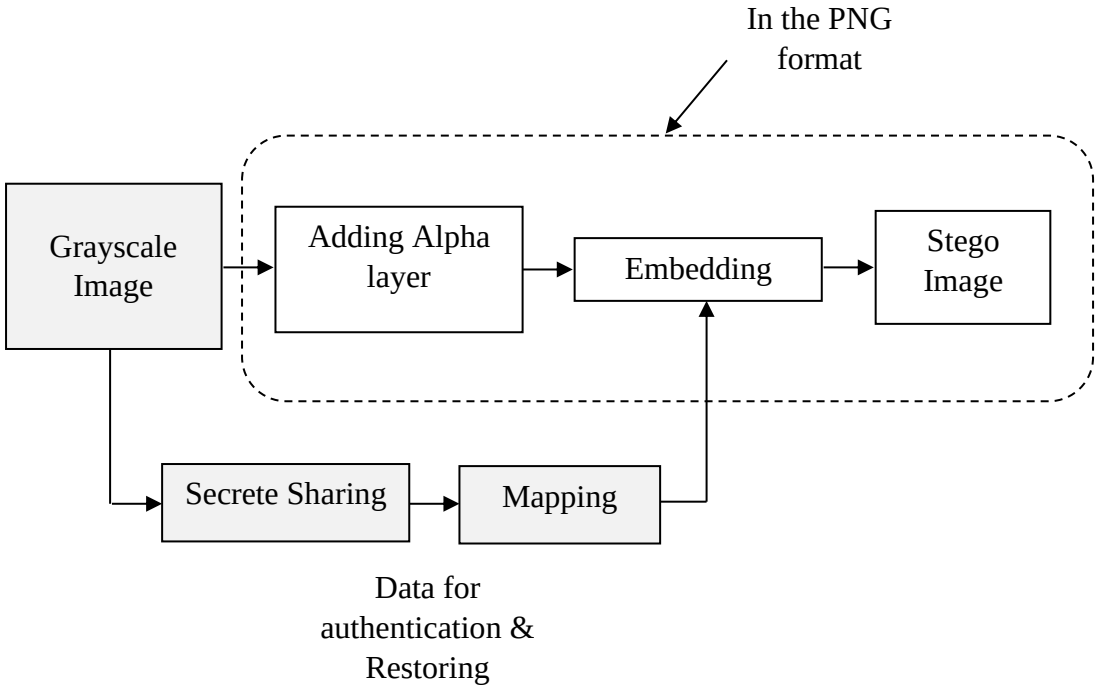


Figure 2 Authentic data inserting method

The suggested method adds an alpha channel before converting the input grayscale picture to the Portable Network Graphics (PNG) format. Data binarization for repair and authentication is completed concurrently. The utmost level of transparency is maintained by embedding this data into the alpha channel. PNG format is used to produce the Stego image. The procedure of embedding genuine data involves the following phases.

Step 1: Cover Image

An 8 bit grayscale image is used as input. We can adapt that grayscale picture to include actual information. The grayscale image that was input contains extensions such as PNG, JPG, BMP, etc. The following equation is used to represent the input grayscale image [10].

Let cover be an initial grayscale picture with size $r * c$ and denoted as:

$$\text{cover} = \left\{ a(x,y) \;\middle|\; \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y) \epsilon \{0,1,2,\dots\dots\dots,255\} \end{matrix} \right\} \quad (1)$$

Where, r is the no. of rows present in a picture and c is the no. of columns present in a picture. Pixel values of an picture are deceits among 0 to 255.

Step 2: Adding an Alpha Channel

In this phase, the alpha channel is introduced. The image's fourth layer is the alpha channel. There is just one in the grayscale picture. For the purpose of transparency, a second layer is applied to the image. The self-mending of tampered data at attacked image regions is contradicted by the fact that the cover image is destroyed first and the original data are no longer accessible for data repairing. This happens following the embedment of the original cover picture data into the image itself for usage in subsequent data restoration. One approach to address this is to copy the original picture data someplace else without altering the cover image itself. This study suggests using a PNG picture's additional alpha channel to contain the original image data in order to accomplish this technique. Nonetheless, the PNG image's alpha channel was first employed to provide the appropriate level of transparency. Moreover, data embedding into the alpha channel will provide an unwelcome opaque effect unpredictable transparency in the PNG image. Mapping the resulting values into a limited range around its extreme value of 255 can almost make the alpha channel plane practically invisible. One approach to reach the intended result is this one. This is how the alpha channel is defined.

$$alpha = \left\{ a(x,y) \;\middle|\; \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y) = 255 \end{matrix} \right\} \qquad (2)$$

The alpha channel in this work is set to be all ones, which means that a white plane will serve as the image's transparent background. Alpha channel is where legitimate data is embedded. The first technique that follows deals with PNG cover image preparation.

Algo. 1: Creation of the cover image i.e. Creation of PNG image

Input: Cover picture

Output: Improved cover picture.png

```
Step 1: Select cover picture as a input
        if (cover picture is PNG)
            {
              Alpha Channel Addition not required
             }
            else
            {
             Alpha Channel addition is required to from PNG picture
            }
Step 2: End
```

Step 3: Binarization and mapping of real data to be used in the secret sharing scheme and for embedding.

Secrete sharing scheme.

Adi Shamir devised the "Secret Sharing" cryptography technique. The main objective of this method is to divide a secret into several separate components needing encryption.
• Assuming S is the secret we wish to encrypt.

• It consists in N pieces: S1, S2, S3,..., Sn.

• After separating the components, the user decides on a number K to decode them and expose the original secret.

• It is chosen so that, should we know less than K parts, we cannot determine the secret S; that is, the secret S cannot be rebuilt with (K – 1) pieces or less.

Assuming we know K or more components from S1, S2, S3,..., Sn, we may easily compute or reconstruct our secret code S. This is generally understood to be a (K, N) threshold system. The main idea of the Shamir's Secret Sharing Algorithm is that for given K points we may construct a polyn equation of degree (K – 1).

As an example:

• For the two sites (x1, y1) and (x2, y2), we may determine a linear poisson ax + by = c.

For the aforementioned three sites, we may also find a quadratic poisson ax2 + bx + cy = d. The aim is to build a polyn of degree (K–1) whereby the secret code is the constant term and the remainder numbers are found at random. Lagrange's Basis Polynom allows one to obtain this constant term from any K points out of the N points this poisson creates.
For instance, let S = 65, N = 4, and K = 2 be the secret codes.
1. First, we construct a polynomial of degree (K – 1) in order to encrypt the secret code.
2. Consequently, let y = a + bx be the polynomial. Our secret code is represented here by the constant portion "a."
3. Choose any random number b, for example, b = 15.
4. Therefore, we have N = 4 points from this polynomial, y = 65 + 15x.
Assign the following four points: (1, 80), (2, 95), (3, 110), and (4, 125). It is evident that any two of these four points may be used to create the starting polynomial, and the constant term an in the resultant polynomial is the necessary secret code.

The cover picture is binarized in this stage. Bit-plane slicing is utilized to binarize the cover picture for embedding purposes, and bit-plane replacement embedding is performed on the cover image.

Eight bit-planes make up grayscale pictures, which may be shown as follows:

$$P_k = \left\{ a(x,y,k) \middle| \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y,k)\ \epsilon\ \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \qquad (3)$$

The input cover picture is an 8-bit/pixel grayscale image. Plus, it contains eight bit-planes. Several bit-planes for a particular grayscale image are displayed in the example that follows [10].

Algo. 2: Binarization (Bit-plane cutting) and shamir secret sharing

Input: Cover picture

Output: 8 bit-planes of cover picture

Step 1: Take cover image

Step 2: cut the cover picture into 8 bit-planes

$$P_k = \left\{ a(x,y,k) \middle| \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y,k)\ \epsilon\ \{0,1\} \end{matrix} \right\} \dots\dots Where: 1 \le k \le 8 \qquad (4)$$

$$P_1, P_2, P_3, P_4, P_5, P_6, P_7\ and\ P_8$$

Step 3: Evaluate polynomial: Generate n shares by evaluating the polynomial P(i , j) distinct non zero points x1,x2,x3 etc.

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

It can be further modified and denoted as P. The data of bit-planes is shared and only P_4 to P_8 bit-planes selected.

Step 3: we only select $P_4, P_5, P_6, P_7\ and\ P_8$ therefore, among bit-planes, these ones have the maximum information level.

Step 4: End

Step 4: Embedding and Mapping

This is the most important stage of the whole operation. This stage incorporates bit-planes 4, 5, 6, 7, and 8 into the alpha channel; the alpha channel is then combined with the grayscale image. Figure 3 offers a clear example of the embedding of actual data in the alpha channel. Bit-plane numbers 4 through 8 are the only ones we take into consideration when embedding real data in the alpha channel. The cover image's highest information is found on bit-planes 4 through 8. Both the alpha channel and the input grayscale picture size ought to be the same [11]-[12].

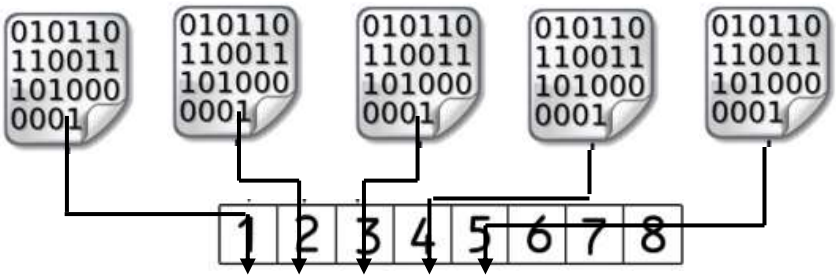


Figure 3 Swapping Alpha channel bit-planes with Authentic information

To obtain the final stego alpha channel, the first five bit-planes of the alpha channel are substituted with real data. The creation of the stego alpha channel is discussed in algorithm 3 below. Bit-plane embedding in the alpha channel is accomplished by this technique [13]-[14].

Algo. 3: Mapping and hiding bit-planes in alpha layer

Input: Alpha layer and bit-planes $P_1, P_2, P_3, P_4, P_5, P_6, P_7\ and\ P_8$

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

Step 1: Select the Alpha Channel (the grayscale image's cover and the alpha channel's size should match).

Step 2: Take $P_4, P_5, P_6, P_7\ and\ P_8$ from slicing of grayscale picture

$$P_k = \left\{ a(x,y,k) \middle| \begin{matrix} 1 \le x \le r, 1 \le y \le c \\ a(x,y,k)\ \epsilon\ \{0,1\} \end{matrix} \right\} \dots\dots Where: 4\ \le\ k\ \le\ 8 \qquad (5)$$

$P_4, P_5, P_6, P_7\ and\ P_8$

Step 3: Alpha layer is a matrix of all 255, cut alpha layer as well

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

$A_1, A_2, A_3, A_4, A_5, A_6, A_7\ and\ A_8$.

Bit-planes of alpha layer comprises of all ones.

Step 4: Stego alpha layer is molded by multiplying binary corresponding multiplier.

$$Stego_{alpha} = P_8 * 2^0 + P_7 * 2^1 + P_6 * 2^2 + P_5 * 2^3 + P_4 * 2^4 + A_3 * 2^5 + A_2 * 2^6 + A_1 * 2^7 \qquad (7)$$

Step 5: End

Step 5: Stego grayscale picture formation

The creation of the stego grayscale picture is the last step in this procedure. To obtain the stego grayscale picture, the input cover image is blended with the stego alpha channel [15].

Combining the stego alpha channel with the cover picture is the focus of Algorithm 4. This method produces a stego grayscale picture as its result.

Algor 4: Developing Stego Grayscale picture

Input: Cover picture and Stego alpha layer

Output: Stego Grayscale picture S

Step 1: Use the Cover picture and Stego Alpha layer.

Step 2: Integrate alpha layer and cover picture together

Step 3: Stego Grayscale picture S= Cover picture + Stego Alpha layer

Step 4: End

II. Verification of Stego picture

This covers the self-repairing process and stego image verification. During this procedure, the calculated authentication data is compared with authentic data that is initially taken from the Stego picture. It is a genuine picture if the two sets of data match. It is not legitimate data if they do not match. Proceed to additional verification and self-repair procedures if a second instance arises.

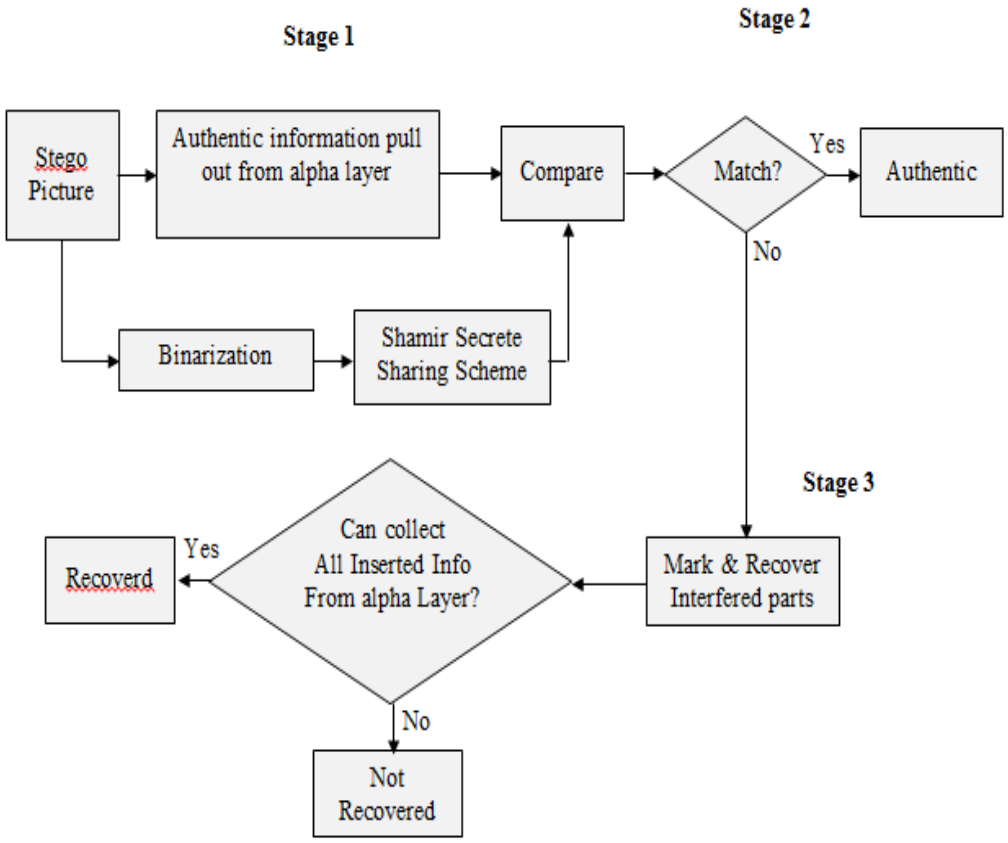


Figure 4 Procedure of authenticating a stego grayscale PNG image

There are three crucial steps in the stego picture authentication process.
Step 1: Taking genuine data out of the alpha channel

Step 2: The stego picture is verified
Stage 3: The original image content self-corrects.
All three phases are depicted in full in Figure 4. Authentic data extraction from the alpha channel is the focus of stage 1. Stage 1 concerns stego picture verification, while Stage 3 focuses on the original image content's self-recovery. Algorithm 5 briefly discusses the previous three steps. The input of this method is stego picture S, and the output is self-repaired image R [16].

Algo. 5: Stego Image Authentication

Input: Stego picture S

Output: Recovered picture R

Stage 1: Extraction of authentic info from alpha layer

Step 1: Initially Take Stego picture

Step 2: Remove alpha layer from stego PNG picture

Step 3: Using bit-plane slicing, take bit-planes one through five from alpha layrs and mark them as S_1, S_2, S_3, S_4 and S_5

Step 4: Now combine all above the alpha layer bit-planes to create a matching and recoverable authentication date, labeled it as a A_{signal}

$$A_{signal} = S_5 * 2^3 + S_4 * 2^4 + S_3 * 2^5 + S_2 * 2^6 + S_1 * 2^7 \quad (8)$$

Stage 2: Confirmation of the stego picture

Step 5: For verification of the true bit-plane slicing (binarization) of stego image (Grayscale data).

Step 6: From above procedure, take final five bit-planes under stated direction. P_4, P_5, P_6, P_7 and P_8

Step 7: Now integrate all above bit-planes to form a confirmation signal for matching, indicate it as a V_{signal}

$$V_{signal} = P_4 * 2^3 + P_5 * 2^4 + P_6 * 2^5 + P_7 * 2^6 + P_8 * 2^7 \quad (9)$$

Step 8: if (A_{signal}= V_{signal})

{

Image is genuine.,

}

else

{

Image is not genuine, Need to recover.

}

Stage 3: Self recovering of original image data

Step 9: In this info is recovered by using A_{signal} and V_{signal}

if $(A_{signal}(i,j) \sim = V_{signal}(i,j))$

{

$R(i,j) = A_{signal}(i,j)$

}

Step 10: Consider the final R as the ideal self-recovered image.

Result Analysis and Discussion:

This study presents simulation data to illustrate the developed algorithms' performance. These algorithms' main objective is to ascertain whether a picture or scanned document is authentic; if not, they seek out the alteration technique and recover data that has been tampered with. In study, each of the previously stated algorithms is explained. The major goals of these algorithms are to find tampered regions on photos, recover original information in tampered areas, embed authentication data in the host file instead of a separate file, and preserve high image visual quality once embedding authentication data in the host file. The stego image's and the restored picture's quality is assessed using many objective criteria. There are two types of objective image quality evaluation (IQA: full reference IQA and no reference IQA. IQA was selected to review the previously mentioned procedural guidelines out of the whole reference. These FR-IQA standards are followed to evaluate the stego and rectified image's quality. Two more metrics designed especially for evaluating built-in algorithms are Embedding Capacity (EC) and Number of Bits Embedded (NBE).

1. Authentication Data embedding

The cover image is drawn from the aadhar card. The image's dimensions are 651*1047.

(a)

(b)

(c)

Figure 5 Authentication info hiding Process of Greyscale Document picture (a) Cover picture (b) Alpha layer + Authentication info (c) Stego picture

Below is a list of the quality parameters for the aforementioned embedding method. The PSNR, MSE, SC, NCC, AD, EC, and NBE are the parameters.

Table 1: Image quality parameters' values for grayscale document image

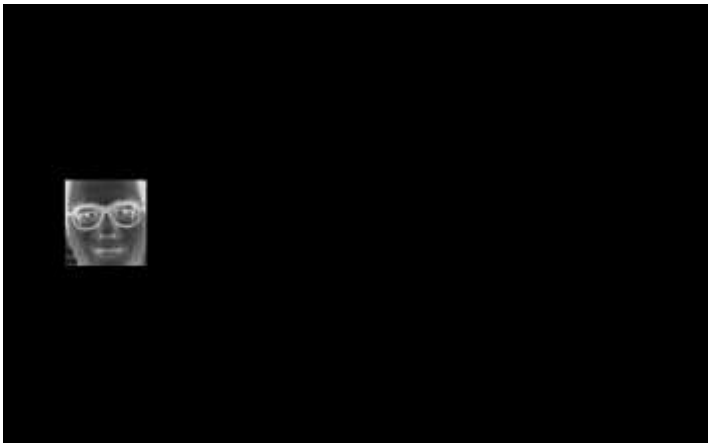
Image Quality Parameter Grayscale document picture	**Values**
Stego Grayscale PSNR in dB	100
Alpha layer PSNR in dB	22.2324
Alpha layer MSE	388.904
Alpha layer SC	0.867587
Alpha layer AD	17.6463
Alpha layer NCC	1.07286
Alpha layer EC	7372800
Alpha layer NBE	4608000

2. External Attacks on the Stego Image, Data Recovery, and Authenticity Verification
Several strategies are used to target the visuals. We have concentrated on purposeful assaults in this study. Following manipulation operations is what is meant by intentional assaults.
i) Cropping Images
ii) Text-based assault
To verify authenticity and retrieve data, algorithm 5 from methodology is now examined for all of the aforementioned threats.

i) Image cropping attack; authenticity check; data recovery.
The face is cropped to erase the proof. The cropped picture is shown in figure 6.

Figure 6 Cropping assault on Greyscale Document picture

Stego images are cropped in order to remove the image's identification. In order to retrieve the original content of the Aadhar card picture, authenticity verification and data recovery are now done over the cropped image.



(a)

(b)

(c)

Figure 7 Authentication, verification and info recovery of Grayscale Document image (a) Removal of Authentication data and verification data (b) Interfered region identification (c) Recovred Image

The following quality metrics are noted in order to assess the restored image's quality. Between the input cover picture and the restored image, quality control is carried out. Table 2 includes all of the quality factors.

Table 2: corrected parameters for picture quality Cropping attack on a grayscale document image

Image Parameter (Quality)Grayscale document Image	**Values**
PSNR (db)	52.0997

Image Parameter (Quality)Grayscale document Image	**Values**
MSE	0.400966
NCC	1.00024
SC	0.999503
AD	0.0798639

ii) Text Attack, Authenticity confirmation and info recovery.

This technique involves inserting text externally onto the picture to assert ownership of the image. Figure 8 shows the text attack.

Figure 8 Text attack on Greyscale Document image

By adding words to the image, anyone may assert ownership of the piece of work. The word "Maher Adel ALDbsawie" is externally put in Figure 8 above to assert the image's ownership.

(a)

(b)

(c)

Figure 9 Grayscale Document image Authentication, verification and info recovery; (a) removal of Authentication data and verification data ; (b)interference region identification; (c) recovered Image

The following quality metrics are noted in order to assess the restored image's quality. Between the input cover picture and the restored image, quality control is carried out. Table 3 includes all of the quality factors

Table 3: corrected parameters for picture quality Cropping attack on a grayscale document image

Image Quality Parameter Grayscale document Image	**Values**
PSNR in dB	56.8344

MSE	0.17767
NCC	1.09823
SC	0.995674
AD	0.057852

Comparison

The literature with different authors in same category of image authentication is compared with proposed method, and comparison is shown in following table 4.

Table 4: Comparison of proposed methods

Sr. No	**Reference**	**Alteration in stego image**	**Interfering revealing ability**	**Restoration capability**	**Work for Color image**	**Data inserting**
1	Reference Wu & Lui [18]	Yes	Yes	No	No	Pixel Flippability
2	Reference Yong & Kot [19]	Yes	Yes	No	No	Pixel Flippability
3	Reference Yong & Kot [20]	Yes	No	No	No	Pixel Flippability
4	Reference Tzeng & Tsai [21]	Yes	Yes	No	No	Pixel replacement
5	Reference Che-Wei Lee [17]	No	Yes	Yes	No	Alpha layer pixel replacement
6	**Proposed Methods**	**No**	**Yes**	**Yes**	**Yes**	**Alpha channel pixel replacement**

Conclusion

Authentication data is integrated into the host file in the methods developed for color and grayscale picture authentication, instead of being stored in a separate data file. It is a serious loss if authentication data, which is kept in a different data file, is misplaced by accident. Nobody is able to determine the authenticity of the photograph in this case. The authenticity verification process becomes more sophisticated with this embedding technique. Instead of embedding authentication data in color or grayscale picture pixels, the developed techniques do it in the alpha channel. The pixels of a color or grayscale image remain intact when using this embedding technique in an alpha channel. The outcomes demonstrate that the stego picture quality is good following the embedding of authentication data. Data about authentication is included in an alpha channel by the created techniques. The image has a transparency effect thanks to the alpha channel. In order to minimize the opaque effect seen in the stego-image, bit-plane slicing is used to insert authentication data into the alpha. the opaque appearance that appears in the stego-image when an alpha channel's bottom bit-planes include authentication data. The research has only found a few number of methods that are effective for grayscale picture data recovery and authentication. The majority of methods in the literature incorporate binary-like data for recovery and authenticity checks. The suggested methods include five grayscale picture bit-planes into an alpha channel. The grayscale image's maximum information is found in these five bit-planes. Maximum grayscale data is corrected throughout the authenticity verification and recovery process. As a consequence, 90% of the corrected image's quality is displayed. The majority of the literature focuses on grayscale and binary picture authentication. While color picture authentication is simple, color image data recovery is more challenging as red, green, and blue plane pixel information is needed for optimal data recovery. Just 8 bit-planes make up the alpha plane. Five bit-planes from red, five bit-planes from green, and five bit-planes from blue cannot be embedded in the alpha channel. Therefore, data restoration capabilities for color images along with authentication are created to address this challenge. To minimize the size, interpolation is first done to the cover picture. Following interpolation, four final bit-planes are created by concatenating fifteen bit-planes; these four bit-planes are then embedded into the alpha channel. Four bit-planes are taken out of the alpha channel during recovery, and fifteen bit-planes are then derived from those four bit-planes to provide the authentication data. After that, gain interpolation is used to adjust the output to the cover image's dimensions. The final result is compared to the verification data; if the two do not match, the authentication data is used to fix the result. The PSNR result demonstrates the good quality of the corrected picture.

References

[1] E. Akhtarkavan, B. Majidi and A. Mandegari, "Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A5 Lattice Vector Quantization," in IEEE Access, vol. 11, pp. 9701-9715, 2023, doi: 10.1109/ACCESS.2023.3238575.

[2] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif and I. Saddique, "An Integrated Image Encryption Scheme Based on Elliptic Curve," in IEEE Access, vol. 11, pp. 5483-5501, 2023, doi: 10.1109/ACCESS.2022.3230096.

[3] X. Wu, N. An and Z. Xu, "Sharing Multiple Secrets in XOR-Based Visual Cryptography by Non-Monotonic Threshold Property," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 33, no. 1, pp. 88-103, Jan. 2023, doi: 10.1109/TCSVT.2022.3199047.

[4] F. Calderon, J. J. Flores and S. Bravo-Solorio, "Watermarks based on Pyramidal Images for Tampering Image Self-Restoration," 2022 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 2022, pp. 1-7, doi: 10.1109/ROPEC55836.2022.10018582.

[5] F. Calderon and S. Bravo-Solorio, "Watermarking Scheme With Bounded-Exhaustive Self-Recovery Approach," 2022 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 2022, pp. 1-11, doi: 10.1109/ROPEC55836.2022.10018607.

[6] F. Ernawan, A. Aminuddin, D. N. E. Phon, E. A. Alsheikh and A. Wibowo, "Self-Recovery in Fragile Image Watermarking Using Integer Wavelet Transform," 2022 IEEE 8th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Melaka, Malaysia, 2022, pp. 21-25, doi: 10.1109/ICSIMA55652.2022.9929127.

[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] Q. Zhang, X. Yuan and T. Liu, "Blind Dual Watermarking Scheme Using Stucki Kernel and SPIHT for Image Self-Recovery," in IEEE Access, vol. 10, pp. 96100-96111, 2022, doi: 10.1109/ACCESS.2022.3204865.

[9] A. Nichal and B. Godbole, "Grayscale Image Authentication with Data Repair Capability," 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Pune, India, 2021, pp. 1-7, doi: 10.1109/SMARTGENCON51891.2021.9645794.

[10] Y. Qiu, Q. Ying, Y. Yang, H. Zeng, S. Li and Z. Qian, "High-Capacity Framework for Reversible Data Hiding in Encrypted Image Using Pixel Prediction and Entropy Encoding," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 9, pp. 5874-5887, Sept. 2022, doi: 10.1109/TCSVT.2022.3163905.

[11] P. Singh, K. J. Devi, H. K. Thakkar and K. Kotecha, "Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT," in IEEE Access, vol. 10, pp. 8974-8993, 2022, doi: 10.1109/ACCESS.2022.3143801.

[12] A. Hanif and M. Doroslovački, "Fully Reversible Steganography with Authentication in Wavelet Domain for Telemedicine Applications," 2021 55th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2021, pp. 881-885, doi: 10.1109/IEEECONF53345.2021.9723196.

[13] A. Bavrina and V. Fedoseev, "Watermarking with recovery capability for HGI image compression," 2021 International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russian Federation, 2021, pp. 1-4, doi: 10.1109/ITNT52450.2021.9649127.

[14] H. Dhane and V. M. Manikandan, "A New Framework for Secure Biometric Data Transmission using Block-wise Reversible Data Hiding Through Encryption," 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), Fez, Morocco, 2021, pp. 1-8, doi: 10.1109/ICDS53782.2021.9626742.

[15] B. Samira, R. H. Lamia and E. B. A. Najoua, "Biometric Template Security Using Watermarking Reinforcement Based Cancellable Transformation," 2021 International Conference on Cyberworlds (CW), Caen, France, 2021, pp. 270-277, doi: 10.1109/CW52790.2021.00052.

[16] Arjun Nichal and Bhalachnadra Godbole, Color Image Authentication with Data Repair Capability, International Journal of Electrical Engineering and Technology (IJEET), 12(6), 2021, pp. 437-452 doi: 10.34218/IJEET.12.6.2021.0042

[17] 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.

[18] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation", IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[19] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier", IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741–744, Dec. 2006.

[20] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving", IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.

[21] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement", IEEE Commun. Lett., vol. 7, no. 9, pp. 443–445, Sep. 2003.