International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Hybrid Approach for Securing Image Tempering in Cloud Storage

[1] Mr. Sachin Sharma, [2]Dr. Brajesh Kumar Singh, [3]Dr. Hitendra Garg

Submitted: 10/09/2023 **Revised**: 22/10/2023 **Accepted**: 08/11/2023

Abstract- The global appeal of leveraging advanced computational infrastructure provided by cloud-based multimedia systems has become increasingly evident. Nevertheless, the security challenges associated with these cloud-based systems, which involve third-party servers, cannot be overlooked. To tackle these security concerns effectively, a proposed solution involves encrypting the data in a way that makes it indecipherable to the cloud data centers. This work introduces an image encryption method built upon the Permutation Ordered Binary (POB) Number System. This technique entails the partitioning of the image into randomly generated shares, which can subsequently be stored in cloud data centers. Furthermore, the proposed method guarantees the integrity of these shares at the individual pixel level. If any unauthorized modifications occur on the cloud servers, the system can accurately detect the altered pixels by leveraging authentication bits and precisely locate the tampered area. This tampered section is also reflected in the reconstructed image, which is accessible to authorized users. The accuracy of tamper detection has been thoroughly evaluated on a pixel-by-pixel basis, demonstrating remarkable effectiveness in a wide range of tampering scenarios.

Keywords: *Permutation ordered binary (POB) number system, secret sharing, encrypted domain*

1. Introduction

Securing image tampering in cloud storage has become an essential concern due to the increasing use of cloud-based storage solutions and the vulnerability of digital images to malicious modifications. Cloud storage offers convenient and cost-effective options for storing and sharing large amounts of data, including images. However, this convenience also brings forth new security challenges, particularly regarding the integrity and authenticity of the stored images.

Image tampering refers to unauthorized modifications or alterations made to digital images with the intention of deceiving viewers or manipulating the visual content. Such tampering can have severe consequences in various domains, including legal, forensics, journalism, and e-commerce. Detecting and preventing image tampering in cloud storage is crucial to maintain trust and ensure the reliability of the stored data.

Cloud storage environments introduce unique challenges for securing image tampering. In traditional local storage setups, users have direct control over their data, whereas in the cloud, the data is entrusted to third-party service providers. This change in accountability necessitates the implementation of strong security measures to safeguard the integrity and genuineness of images archived in the cloud.

One of the primary concerns in securing image tampering in cloud storage is the prevention of unauthorized access and modification of the images. Cloud storage systems need to incorporate robust authentication and access control protocols to guarantee that solely authorized users can access and make changes to the stored images. Additionally, encryption techniques can be employed to protect the images from unauthorized interception and tampering during transmission and storage.

An additional crucial element involves identifying and pinpointing altered sections within the images. Diverse methods, such as digital forensics, image processing, and machine learning algorithms, are used for this purpose. can be leveraged to identify inconsistencies or irregularities in image content that indicate tampering. These techniques analyze image metadata, pixel-level analysis, and statistical features to detect tampered regions accurately.

Furthermore, secure image hashing and watermarking methods can be applied to embed unique digital signatures or metadata into the images. This allows for the verification of image authenticity and integrity at a later stage, even if the images have been tampered with. By comparing the computed hash values or extracting watermarks from the stored images, one can validate their integrity and detect any tampering attempts.

In conclusion, securing image tampering in cloud storage is crucial to maintain trust, integrity, and authenticity of stored

[1]*Research Scholar AKTU Lucknow,India*
sachin.sharma@gla.ac.in
[2] *Associate Professor FET,RBS College Bichpuri,Agra,India*
brajesh1678@gmail.com
[3]*dept. of CE&A GLA University Mathura, India*
hitendra.garg@gla.ac.in

images. Robust authentication, access control, encryption, tampering detection, and watermarking techniques are essential components of a comprehensive security framework for cloud-based image storage. By implementing these measures, users and organizations can mitigate the risks associated with image tampering and ensure the reliability of their stored visual data.

1.1 Image manipulation, forgery and tempering

Image manipulation, forgery, and tampering are terms used to describe various forms of unauthorized alterations or modifications made to digital images. Each term refers to a specific type of manipulation with different intentions and techniques involved. Here's an explanation of each term:

Image Manipulation- Image manipulation refers to the deliberate modification of digital images to achieve a desired effect or aesthetic appeal. It can involve adjusting various image attributes, such as color, contrast, brightness, and sharpness, to enhance the visual quality or create a specific artistic effect. Image manipulation is commonly performed using image editing software like Adobe Photoshop or GIMP. In the context of digital forensics or authenticity verification, image manipulation can also refer to any deliberate alteration made to deceive or mislead viewers.

Image Forgery- Image forgery involves creating or modifying an image with the intention of deceiving or misleading viewers. It typically involves the creation of counterfeit or fake images that appear authentic. Forgery can take various forms, such as fabricating entire images, cloning or copying elements from one image to another, or altering specific regions within an image. The goal of image forgery is often to create a false narrative, manipulate evidence, or misrepresent information. Detecting image forgery is an important task in fields such as forensics, journalism, and legal proceedings.

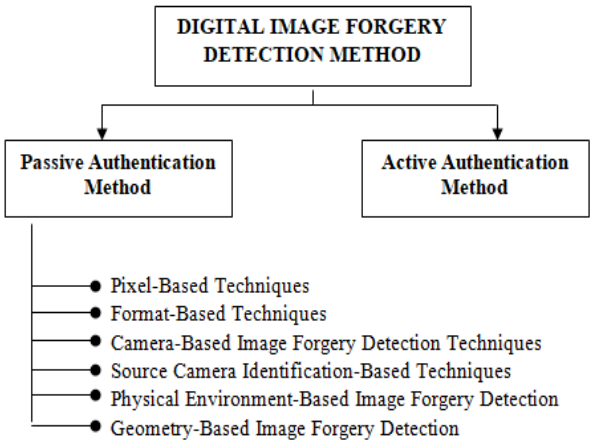
Image Tampering: Image tampering pertains to the unauthorized modification or change in digital images without the knowledge or consent of the image owner or the intended audience. Tampering can involve inserting or removing objects, manipulating the content, or modifying specific regions within an image to misrepresent information or deceive viewers. Tampering can be performed for various reasons, including photo manipulation for personal or malicious purposes, falsifying evidence, or spreading misinformation. The detection and pinpointing of image tampering are essential for upholding the integrity and authenticity of digital images.

In all these scenarios, the use of digital forensics techniques, image processing algorithms, and machine learning methodologies is common for detection. and analyze inconsistencies, anomalies, or traces left by the manipulation or tampering process. These techniques involve examining pixel-level analysis, metadata analysis, image hashing, watermarking, and statistical analysis to identify signs of manipulation or tampering within the images.

In general, image manipulation, forgery, and tampering underscore the significance of upholding the authenticity, integrity, and reliability of digital images, particularly in fields like forensics, journalism, and legal proceedings, where precise representation and evidence hold great importance.

1.2 Digital image forgery detection method

The detection of digital image forgery can be classified into two categories: active methods (non-blind) and passive methods (blind), depending on whether the original image is available or not [1][2][3][4].



1.2.1 Active Authentication Method

This technique involves the insertion of data during the creation of an image, which can later be used to identify the image's source or detect potential alterations. Active authentication methods can be divided into two categories: digital watermarking [21], [22] and digital signatures [23]. Digital watermarking embeds a bit pattern into a digital image during acquisition or processing, while digital signatures incorporate certain information derived from the same image into the image itself. This approach offers the advantage of lower computational costs, and if information about the original image is available, fraud detection becomes straightforward. However, the drawback is that these methods require embedding into images at the time of capture using specialized hardware, and prior knowledge of the image is essential for validation.

Passive authentication involves no additional data insertion during image creation. Intrinsic patterns from imaging devices or processing tools are inherent, remaining constant in genuine images. Any alteration disrupts these patterns. Also known as blind authentication, it relies solely on image features, not needing the original for integrity verification. It's inactive, lacking real-time data like watermarks or fingerprints. Manipulation distorts the statistical patterns in authentic images, often unnoticed visually. This leads to identifying inconsistencies using simple image processing methods. Passive detection methods categorize into pixel, format, camera, source camera ID, physics, and geometric-based approaches. A brief description of each classification in given below.

(a) Pixel-Based Techniques

Pixel-based techniques encompass the identification of statistical irregularities at the pixel level and the examination of pixel-level relationships that arise in the spatial or modified domain during the tampering process. Generally, there exist four specific categories of pixel-based forgery recognition methods: copy-move, splicing, resampling, and statistical analysis.

(b) Format-Based Techniques

The JPEG format plays a primary role in this technique. It leverages the measurable relationships resulting from specific lossy compression to detect image forgeries. These methods can be categorized into JPEG quantization, Double JPEG, and JPEG blocking. When an image is in a compressed format, it extremely difficult to differentiate the original and forged image. However, using format based techniques, it is possible to detect forged images out of available compressed images.

(c) Camera-Based Image Forgery Detection Techniques

This process detects alterations introduced during the image creation by examining variations introduced by different stages of the imaging process, This encompasses a range of techniques, including quantization, color correlation, gamma correction, white balance, filtering, and JPEG compression. Various factors, such as chromatic aberration, color filter array, camera response, and sensor noise imperfections, can be employed to detect specific alterations made by the camera.

(d) Source Camera Identification-Based Techniques

To detect tampering, the camera's image capture specifications are employed, which involve analyzing factors such as sensor noise, color filter array interpolation, and deviations in the camera lens.

(e) Physical Environment-Based Image Forgery Detection

In natural photography or when capturing a realistic image, varying lighting conditions are typically encountered. The variations in the original image's brightness and contrast can serve as indicators to identify or detect any manipulation aimed at creating an altered image. Analyzing the differences in lighting between the tampered image and the original image can be one of the most effective methods for identifying image forgery.

Let's take the example of a manipulated image depicting two individuals walking on a beach, where the original images of these two people were originally captured separately in different settings. By examining the lighting conditions in the manipulated image, we can establish whether it is authentic or a forgery.

(f) Geometry-Based Image Forgery Detection

When taking a photograph, the camera lens focuses light from an object. This incoming visual information hits the image sensor chip, which breaks it down into numerous individual pixels. The sensor then quantifies the color and brightness of each pixel and stores this information as numerical values. These measurements are all relative to the camera's central or principal point projected onto the image plane.

If the camera's principal point on the image plane is positioned close to the center of the image, the result is an unaltered, unadulterated image. However, any movement of the object, shifts in the image's translation, or the joining of different image segments to create a composite image will alter the location of the principal point within the image.. The internal metric parameters like skew, aspect ratio, focal length, principal point recovered from a non-tampered image should be varying across the image and it is an evidence to notice the tampering. Hence it is possible to develop forgery detection algorithms by applying projective geometry principles. Thus it is a multidimensional a approach in forgery detection. The identification of copied regions in manipulated images can often occur without requiring a reference to the original image [5, 6]. In instances of copy-move forgery (Table -1), this manipulation involves duplicating and inserting a segment of an image within the same image, a phenomenon also known as merged images [7].

Table-1: Evaluation of diverse methods for detecting copy-move forgery.

Authors	Year	Features Extracted	Classifier used	Limitations
Zhao and J.Guo [24]	2013	DCT applied to blocks that have overlapping regions.	Arranging items in a sequence based on their lexicographical order.	Lacking computational speed.
P.Xunyu and L.Siwei [25]	2011	Distinctive features identified in an image using the Scale-Invariant Feature Transform (SIFT) algorithm.	K-means	Inappropriate for use with small block sizes.
B. Mahdian, S.Saic [26]	2008	Blur moment invariants are numerical quantities that remain unchanged despite the presence of blurring effects in images.	K-Dimensional tree	The approach yields a substantial number of incorrect positive results
G. Muhammad, M. Hussain and G. Bebis [27]	2012	Dyadic wavelet transform decomposes signals/images into scales, orientations, analyzing frequencies/patterns across resolutions.	Categorization through the application of threshold values.	Not universally suitable for processing color data.
Li, J., Li, X., Yang, B., Sun, X [28]	2015	VIFeat software involves robust model fitting to handle outliers and noise in data.	K NN	Limited processing speed
Lee, J.C., hang, C.P., et.al.[29]	2015	Histogram of Oriented Gradients (HOG)	Lexicographal order	Not suitable for high rotation and scaling
Zhu, Y., Shen,et. Al.[30]	2016	ORB features	FAST keypoints and the ORB features	Reduced speed with high-resolution images.

Huang, Det.al[31]	2017	FFT SVD, and PCA	comprehensive exploration.	Elevated precision in detection
Popescu, A. and Farid, H. [32]	2004	PAC(Principle Component Analysis)	Accuracy, sensitivity, and false positive rate	Incapable of identifying spliced regions.

1.3 POB Number system

The POB (Pattern of Bits) Number System is a method used to encode and analyze the patterns of bits within digital images. It assigns a unique numerical value to each distinct binary pattern found in an image, allowing for efficient representation and analysis.

For example, let's consider a grayscale image represented by pixel values ranging from 0 to 255. We convert each pixel value into its binary representation. Suppose we have an 8-bit grayscale image, where each pixel is represented by 8 bits.

These POB numbers provide a compact representation of the patterns of bits within the image. By comparing the POB numbers of different regions or comparing the POB numbers of an image before and after potential tampering, inconsistencies or variations can be detected, indicating the presence of tampering.

The use of the POB Number System allows for efficient analysis of binary patterns in images, enabling applications such as image retrieval, content-based image analysis, and secure cloud-based image tampering detection and localization.

The study described in reference [40] introduced an image encryption technique relying on the permutation ordered binary (POB) number system. In this approach, the image data was fragmented into entirely randomized shares, which could be stored in a cloud data center. Moreover, this devised method accomplished pixel-level authentication.

Notably, the scheme had the ability to accurately detect tampering at the pixel level if any modifications were performed on the cloud server, thanks to the utilization of authentication bits.

1.3.1 Property of POB number System

The POB (Pattern of Bits) Number System possesses several properties that make it useful for encoding and analyzing patterns of bits within digital images. Some key properties of the POB number system are:

1. Uniqueness: Each distinct binary pattern in an image is assigned a unique numerical value. This property ensures that different patterns are represented by different POB numbers, allowing for reliable identification and comparison of patterns.

2. Compactness: The POB number system provides a compact representation of the patterns of bits within an image. Instead of storing or comparing the entire binary pixel data, the POB numbers can be used, significantly reducing the storage and computational requirements.

3. Preservation of Similarity: The numerical values assigned to the patterns in the POB number system are typically designed to preserve the relationships and similarities between different patterns. Patterns that are similar or share common features often have numerically close POB numbers, allowing for meaningful comparisons and analysis.

4. Efficient Analysis: The use of POB numbers enables efficient analysis of patterns in digital images. By comparing the POB numbers of different regions or comparing the POB numbers of an image before and after potential tampering, inconsistencies or variations can be detected, aiding in tasks such as tampering detection and localization.

5. Applicability: The POB number system can be applied to various types of digital images, including grayscale or color images. It is not limited to a specific image format or size, making it versatile for different image analysis tasks.

6. Robustness: The POB number system is designed to handle noise or minor variations within the binary patterns. It can tolerate slight differences caused by compression, noise, or minor image alterations, ensuring reliable and robust pattern analysis.

7. Computational Efficiency: The POB number system can be computed efficiently, requiring minimal computational resources. This property is advantageous in scenarios where real-time processing or analysis of large image datasets is required.

Overall, the properties of the POB number system make it a valuable tool for encoding, comparing, and analyzing patterns of bits in digital images. Its uniqueness, compactness, preservation of similarity, and computational efficiency

contribute to its applicability in various image analysis tasks, including Reliable image tampering detection and localization in a secure cloud environment.

2. Related Work

To ensure image privacy, since the cloud servers may not be reliable, a solution is implemented by dividing the image into multiple shares. Each share alone doesn't expose any information, but when combined, they allow the original image to be reconstructed [21].

In their publication [22], Sreekumar and colleagues presented a secret sharing method that employs the Permutation Ordered Binary (POB) Number System. This approach enables the division of a secret into multiple shares (n shares), where each share comprises POB-values representing segments of the secret. To recover the original secret, the binary POB-values within the shares are converted to decimal, and these values are then combined to reconstruct the original secret.

The article [10] examined the verification of content in the context of server-proxy-user, involving the utilization of intermediate proxies positioned between multimedia servers and users.

The article [11] suggests that by employing certain methods and techniques, it is possible to acquire information about the manipulation of the cover image, as well as identifying the specific areas that have been tampered with.

In reference [12], the author discusses how schemes, in addition to tamper localization, can be utilized to acquire details about the manipulation of the cover image.

In the study described in reference [13], the researchers presented authentication methods that make use of watermarking techniques to ensure the integrity of the unencrypted original data. They carried out a comprehensive assessment of authentication schemes for both non-scalable and scalable multimedia streams.

The author of the paper [14] performed a thorough analysis of authentication techniques applicable to both non-scalable and scalable multimedia streams.

In the study cited as reference [15], a weighted-sum function was utilized to incorporate authentication bits into a block, leading to a reduction in the number of authentication codes and an enhancement in the protected image's quality. The comparison of these authentication bits with the least significant bits (LSBs) of the received image allows for the detection of any modified pixels within the image. Nonetheless, a limitation of these methods arises when embedding the watermark or authentication bits in the LSBs, as it necessitates a trade-off between imperceptibility and authentication capacity.

The authors of Paper [19] have investigated reversible watermarking algorithms and introduced a tamper localization technique that enables the targeted rejection of altered images. In the paper [21], an innovative watermarking method based on chaos has been introduced, utilizing chaotic maps for the purpose of tamper detection.

The content in the paper [20] elaborates on the possibility of intruders targeting the encrypted shares stored by these servers, even without any knowledge of the actual content. Such attacks can jeopardize the integrity of the shares and potentially disrupt the retrieval of the secret image.

A publication referenced as [23] illustrates the implementation of a secure distribution technique that combines the principles of the POB Number System and the Chinese Remainder Theorem.

In the work by Abhishek Parakh and Subhash Kak in 2009, they discuss the utilization of a data partitioning scheme to securely distribute data randomly across the network. This approach mandates that an authentic entity possesses a login password to reconstruct the data. This method finds applications in sensor networks [7-9] and Internet Voting Protocols (IVP).

Zhu and colleagues in their study [30] explored copy-move forgery detection employing scaled ORB, which proved effective for handling geometric transformations. Nevertheless, it demonstrated reduced performance when processing high-resolution images.

Huang and co-authors in their research [31] introduced a robust copy-move forgery detection technique employing FFT, SVD, and PCA. This method is particularly well-suited for images with substantial JPEG compression.

Popescu and Farid introduced a method in their paper [32] that recommended the use of Principal Component Analysis (PCA) to represent images as vectors following a grayscale transformation. This approach facilitated the distinction of minor variations caused by noise. Furthermore, it proved to be highly effective for grayscale images and demonstrated its proficiency in forgery detection. This suggested technique also led to a simplification of the overall process.

Al-Sawadi and colleagues [33] conducted research focused on identifying counterfeit images using the Local Binary Pattern (LBP) technique. Initially, the image is converted to grayscale. Subsequently, block-pairs with the smallest distances are chosen using histogram distance calculations within these blocks. The main candidates are determined by considering the

retained block pairs, which encompass three color components. This approach led to a decrease in false positive rates when compared to alternative methods. Nevertheless, it's worth noting that the proposed technique is not suitable for transformation operations like rotation and scaling.

Bayram and his team [34] utilized the Fourier-Mellin Transform (FMT) for detecting manipulated images. This technique involves dividing the image into smaller blocks and then computing the Fourier Transform for each block. The method demonstrated effectiveness in handling geometric alterations such as scaling and slight rotations, specifically within a range of 10% for scaling and up to 10 degrees for rotation.

Shao and colleagues [35] employed a technique involving circular window expansion and phase correlation to achieve their goals. This method involves obtaining the phase matrix of expanded blocks through Discrete Fourier Transform (DFT). It has the capability to detect regions within the image that have been copied, rotated, and moved. The method demonstrated its effectiveness in scenarios involving rotation, blurring, JPEG compression, and variations in luminance. However, it's worth noting that the method was found to be time-consuming and did not perform adequately when dealing with scaling operations.

Tai and colleagues [36] implemented pseudocode for a detection and smoothing technology as part of an efficient self-embedding watermarking scheme.

Wang and collaborators [37] introduced an image self-recovery approach involving a watermark self-embedding algorithm within a hierarchical detection and recovery framework. Nevertheless, the drawback of these reversible watermarking techniques lies in their inability to ensure both accurate restoration of the original image and reliable identification of tampered areas simultaneously.

N. Sasikaladevi and her coauthors [38] employed a lightweight model called SNAP (SeNsitive image Authentication Protection) to achieve compression without data loss, thus conserving storage space, and to enhance encryption speed while maintaining security. However, the technique's design did not adequately consider the intricacies associated with medical images.

The approach outlined in reference [39] introduced a semi-fragile watermarking technique that includes added image recovery capabilities. This methodology bolsters security by establishing a correlation between the embedded watermark and the approximate sub-wavelet transform. Furthermore, the method incorporated a lossless compression algorithm and a low-pass version of BCH coding to enhance the image recovery capacity [41][42]

When it comes to forgery, it is possible to authenticate each share at a detailed level, examining individual pixels. By doing so, it becomes feasible to pinpoint the exact locations of forged websites and even detect them in the reconstructed image obtained from the authentic source. The suggested approach effectively addresses the difficulties associated with detecting tampering in the encrypted domain and addresses the following issues [43][44].

1. Image recovery without loss: The proposed scheme, utilizing the POB number system, allows the authentication bits to be appended to the POB numbers associated with the shares' POB values. This approach ensures that there is no loss of information in the shares, resulting in an exact and undistorted recovery of the image.

2. Blind authentication: The authentication process for the encrypted shares does not require any additional information. It can be performed independently. In case any share is subjected to an attack, the alteration of authentication bits will indicate the tampering and accurately pinpoint the modified areas [45][46].

3. Precise localization of tampered pixels: Multiple authentication algorithms operating at the pixel level, considering the location, neighborhood, and value of the encrypted shares, enable accurate localization of tampered regions within the image [47][48].

3. Proposed Work

The security of data stored across numerous cloud data centers is prone to vulnerabilities. Hence, in the scheme presented, the image shares undergo encryption to ensure that image information remains undisclosed to third-party servers. The core concept of this scheme is depicted in Figure 1. The Permutation Ordered Binary (POB) number system is employed to create these shares, ensuring a fully random distribution [49][50].

Algorithm-1: Procedure of Proposed work

Sender End

// Generate Horizontal Partitions of original image

segments_of_image = generate_Horizontal_Partitions (Image);

//Add Sequence bits with each partitions

segments_of_image= addSequenceBits(segments_of_image$_i$);

// Generate POB shares for each partition

pobShares$_i$ =generate_POB_shares(segments_of_image$_i$);

// Put all POB shares over the different cloud server center

store(cloud_server_centers, pobShares);

Receiver End/ Authentic Entity

//Tampered Detection for each partition in cloud-based POB share:

segments_of_image =tamparedDetection (cloud_server_centers, segments_of_image$_i$);

//Arrange all partitions according their sequence, remove sequence number and reconstruct original Image

image = reconstructImage(segments_of_image);

Algorithm-2: Procedure of Generate POB shares

Generate POB shares (segments_of_imagei)

{

//Put segments_of_image$_i$ variable S

1. For each pixel (i, j) in the secret image:

1.1. Calculate Tm by dividing the pixel value S (i, j) by 2^u and taking the result modulo 2, where u ranges from 7 to 0. This step computes the binary equivalent of the pixel value.

2. For each bit position m from 0 to 7:

2.1. If Tm is 1:

2.1.1. If the count of occurrences of 1 in the binary representation of Tm is even, set Am to 1.

2.1.2. If the count of occurrences of 1 in the binary representation of Tm is odd, set Am to 0.

2.2. If Tm is 0, set Am to a random value of 0 or 1.

3. Compute Bm by performing bitwise XOR between Tm and Am for each bit position m.

4. Generate S1(i, j) by computing the equivalent POB value for the A vector obtained from the previous steps.

5. Generate S2(i, j) by computing the equivalent POB value for the B vector obtained from the previous steps.

6. Return the two POB shares S1 and S2.

}

It create two shares of a secret segments of image by using a specific process involving the binary representation of pixel values and some operations based on counting the occurrences of 1s. The shares are generated using the calculated A and B vectors, and the equivalent POB values for these vectors are used to create the final shares [51][52].

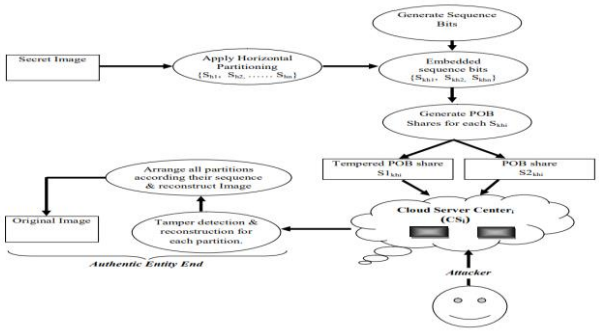
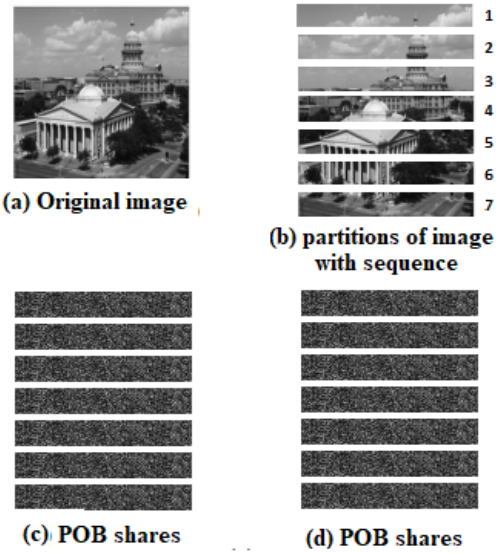


Fig-1: Proposed approach for Securing Image Tempering in cloud storage

For instance, when encrypting the test image into multiple partitions, the only additional memory requirement is that of each secret share stored on remote cloud servers. We create horizontal partitions (illustrated in figure 3(b)) of the original image (depicted in figure 3(a)). Random POB shares for all segments are generated and stored on different cloud data centers, as shown in figures 3(c) and 3(d), respectively. By rearranging all partitions according to their sequences, we reconstruct the original image, as presented in figure 3(e) and 3(f). Consequently, the proposed scheme effectively addresses the issue of image confidentiality at cloud data centers [53][54].



(a) Original image

(b) partitions of image with sequence

(c) POB shares

(d) POB shares

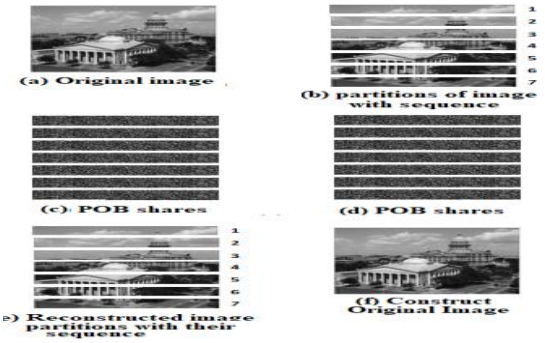


Fig-2 : Step-wise output of approach: (a) Original image (b) partitions of image with sequence (c)(d) Reconstruct image partitions with their sequence (f) Construct original Image

4. Security Analysis

The proposed approach ensures both the confidentiality and integrity of data within a cloud-based framework. Data confidentiality is guaranteed by the use of POB shares derived from the original image segments. These shares are devoid of any revealing information and are entirely random, making them suitable for secure distribution across cloud data centers. Additionally, the scheme offers an integrity check through authentication modes tied to segment levels and their sequence bits, serving as authentication markers. By implementing authentication at the segment level, the scheme has the ability to identify any tampered segments even if they are present within the shares.

Only an authorized user who possesses all the secret shares can successfully reconstruct the original image. The scheme provides protection against image reconstruction when an insufficient number of shares is available. In the most challenging scenario, where an unauthorized user manages to obtain all secret shares, they would also need the specific sequence number to decode a POB value into its corresponding POB number. As this number is exclusively available to a legitimate entity, an attacker without knowledge of the number of 1s cannot reconstruct the original image, even if they possess all the shares. Consequently, any potential information leakage related to the original image is restricted to what might be contained within the shares. The article also provides a quantitative demonstration to validate the genuine randomness of the secret shares and the minimal significance of the information retained within them.

5. Conclusion & Feature Work

This article introduces an effective technique for safeguarding the confidentiality and integrity of multimedia data within a cloud-based framework. The method leverages a number system rooted in Permutation Ordered Binary (POB) to generate multiple random shares of all the divisions of the original image, thus upholding the image's confidentiality.The study concludes that pixel-level authentication produces superior results compared to neighborhood-based authentication. Notably, the proposed scheme holds an advantage over other existing methods as it conducts authentication at the pixel level, obviating the need for additional shares to verify the integrity of a particular share. Future research may involve implementing and testing the scheme against a wider range of attacks while reducing the probabilities of false acceptance and rejection, with the ultimate goal of achieving improved results.

References:

[1] Christian Riess and Tiago Jose de Carvalho,"Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions On Information Forensics And Security, vol. 8,2013

[2] Tu K.Huynh, Thuong Le-Tien, Khoa V.Huynh, Sy C.Nguyen A Survey on Image Forgery Detection Techniques, The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), DOI 978-1-4799-8044-4/15

[3] U. Tembe, S. Thombre, "Survey of Copy-Paste Forgery Detection in Digital Image Forensic", International Conference on Innovative Mechanisms for Industry Applications (2017)

[4] Asghar K, Habib Z, Hussain M (2017) Copy-move and splicing image forgery detection and localization techniques: a review. Aust J Forensic Sci 49(3):281–307

[5] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," Australian Journal of Forensic Sciences, vol. 49, no. 3, pp. 281–307, 2017. DOI: 10. 1080/00450618.2016.1153711.

[6] Gajanan K. Birajdar, Vijay H. Mankar Digital image forgery detection using passive techniques: A survey, Digital Investigation 10(3): 226- 245 (2013).

[7] Bo Xu, Guangjie Liu, and Yuewei Dai , "Detecting Image Splicing Using Merged Features in Chroma Space", the Scientific World Journal",2014.

[8] T. Yuan, S. Zhang, Secure fault tolerance in wireless sensor networks, in: CITWORKSHOPS'08: Proceedings of the 2008 IEEE Eighth International Conference on Computer and Information Technology Workshops, 2008, pp. 477–482.

[9] W. Zhang, G. Cao, T.L. Porta, Data dissemination with ring-based index for sensor networks, in: IEEE International Conference on Network Protocol,November 2003.

[10] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. 2015. Security in cloud computing: Opportunities and challenges. Inf. Sci. 305 (2015), 357–383

[11] Charles Asmuth and John Bloom. 1983. A modular approach to key safeguarding. IEEE Transactions on Information Theory 29, 2 (1983), 208–210.

[12] Gaurav Bhatnagar, Q. M. Jonathan Wu, and Pradeep K. Atrey. 2013. Secure randomized image watermarking based on singular value decomposition. ACM Trans. Multimedia Comput. Commun. Appl. 10, 1, Article 4(Dec. 2013), 21 pages. http://doi.acm.org/10.1145/2542205.2542207

[13] V. P. Binu and A. Sreekumar. 2014. Generalized secret sharing using permutation ordered binary system. CoRR abs/1407.3609 (2014). http://arxiv.org/abs/1407.3609.

[14] George Robert Blakley. 1979. Safeguarding cryptographic keys. In Proceedings of the National Computer Conference. 313–317.

[15] Dan Bogdanov. 2007. Foundations and properties of shamirs secret sharing scheme research seminar in cryptography. University of Tartu, Institute of Computer Science.

[16] Marco Botta, Davide Cavagnino, and Victor Pomponiu. 2014. Protecting the content integrity of digital imagery with fidelity preservation: An improved version. ACM Trans. Multimedia Comput. Commun. Appl. 10, 3, Article 29 (April 2014), 5 pages. http://doi.acm.org/10.1145/ 2568224.

[17] Zouhair Chiba, Noureddine Abghour, Khalid Moussaid, Amina El Omri, and Mohamed Rida. 2016. A survey of intrusion detection systems for cloud computing environment. In Proceedings of the International Conference on Engineering & MIS (ICEMIS). IEEE, 1–13.

[18] MP Deepika and A Sreekumar. 2016. A novel secret sharing scheme using POB number system and CRT. Int. J. Appl. Eng. Res. 11, 3 (2016), 2049–2054.

[19] Robert H. Deng and Yanjiang Yang. 2009. A study of content authentication in proxy-enabled multimedia delivery systems: Model, techniques, and applications. ACM Trans. Multimedia Comput. Commun. Appl. 5, 4, Article 28 (Nov. 2009), 20 pages. http://doi.acm.org/10.1145/1596990.1596992.

[20] Jiri Fridrich and Miroslav Goljan. 1999. Protection of digital images using self embedding. In Symposium on Content Security and Data Hiding in Digital Media. Newark, NJ.

[21] Singh, P.,Chadha, R.S.:Asurvey of digital watermarking techniques, applications and attacks. IEEE Int. Conf. Ind. Inform. 2, 165–175 (2013)

[22] I. J. Cox, M. L. Miller, J. A. Bloom and C. Honsinger, "Digital watermarking", San Francisco: Morgan Kaufmann, vol. 1558607145, (2002).

[23] Lu, C., Liao, H.M., Member, S.: Structural digital signature for image authentication: an incidental distortion resistant scheme. IEEE Trans. Multimed. 5, 161–173 (2003)

[24] Zhao and J.Guo,"Passive forensics for copy-move image forgery using a method based on DCT and SVD",International Conference on forensic science,pp.158-166,2013.

[25] P.Xunyu and L.Siwei,"Region duplication detection using image feature matching",IEEE Transactions on Information Forensics security,pp.857- 67,2011

[26] B.Mahdian,S.Saic,"Blind methods for detecting image fakery",IEEE Int. Carnahan conference on security technology,pp.280-6,2008.

[27] G.Muhammad,M.Hussain and G.Bebis,"Passive copy-move forgery detection using undecimated dyadic wavelet transform",Digital investigation,pp.49-57,2012.

[28] Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detectionscheme. IEEE Trans. Inf. (2015)

[29] Lee, J.C., Chang, C.P., Chen, W.K.: Detection of copy-move image forgery using histogramof orientated gradients. Inf. Sci. (Ny) 321, 250– 262 (2015)

[30] Zhu, Y., Shen, X., Chen, H.: Copy-move forgery detection based on scaled ORB. Multimed.Tools Appl. 75, 3221–3233 (2016)

[31] Huang, D., Huang , C., Hu,W.: Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimed. Tools Appl. 76(1), 1509–1530 (2017)

[32] Popescu, A. and Farid, H. (2004), "Exposing Digital Forgeriesby Detecting Duplicated Image Regions", Tech. Rep. TR2004- 515,Dartmouth College, Computer Science, Hanover

[33] Al-Sawadi, M. Mohammad, G. Hussain, M. Bebis, G. (2013),"Copy- Move Image Forgery Detection Using Local Binary Patternand Neighborhood Clustering", Modelling Symposium (EMS),2013 European, (20-22 Nov. 2013), Manchester, pp. 249 – 25.

[34] Bayram, S. Sencar, T. Memon, N. (2009), "An Efficient andRobust Method forDetecting Copy-Move Forgery", in Proceedingof the IEEE International Conference on Acoustics, Speech, andSignal Processing (ICASSP '09), pp. 1053–1056, Taipei, Taiwan.

[35] Shao, H. Yu, T. Xu, M. Cui, W. (2012), "Image regionduplication detection based on circular window expansion andphase correlation", Forensic Science International, vol. 222, no. 1–3, pp. 71–82.

[36] Singh D, Singh SK (2006) Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. J Vis Commun Image Represent 38(Jul 2016):775–789

[37] Tai W-L, Liao Z-J (2018) Image self-recovery with watermark self-embedding. Signal Process. Signal Process Image Commun 65(Jul. 2018):11–25

[38] Sasikaladevi N, Geetha K, Mahalakshmi N et al (2019) SNAP-compressive lossless sensitive image authentication and protection scheme based on Genus-2 hyper elliptic curve. Multimed Tools Appl 78: 26163–26179

[39] Chamlawi R, Khan A (2010) Digital image authentication and recovery: Employing integer transform based information embedding and extraction. Inf Sci 180(Dec. 2010):24

[40] Afjal MI, Mamun MdA, Uddin MdP (2019) Band reordering heuristics for lossless satellite image compression with 3D-CALIC and CCSDS. J Vis Commun Image Represent 59(Feb. 2019):514–526.

[41] Kumar, Vimal, and Rakesh Kumar. "A cooperative black hole node detection and mitigation approach for MANETs." In Innovative Security Solutions for Information Technology and Communications: 8th International Conference, SECITC 2015, Bucharest, Romania, June 11-12, 2015. Revised Selected Papers 8, pp. 171-183. Springer International Publishing, 2015.

[42] Kumar, V., Shankar, M., Tripathi, A.M., Yadav, V., Rai, A.K., Khan, U. and Rahul, M., 2022. Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme. Journal of Scientific & Industrial Research, 81(10), pp.1061-1072.

[43] Kumar, V. and Kumar, R., 2015. An adaptive approach for detection of blackhole attack in mobile ad hoc network. Procedia Computer Science, 48, pp.472-479.

[44] Kumar, V. and Kumar, R., 2015, April. Detection of phishing attack using visual cryptography in ad hoc network. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1021-1025). IEEE.

[45] Kumar, V. and Kumar, R., 2015. An optimal authentication protocol using certificateless ID-based signature in MANET. In Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3 (pp. 110-121). Springer International Publishing.

[46] Kumar, V. and Kumar, R., 2017. Prevention of blackhole attack using certificateless signature (CLS) scheme in MANET. In Security Solutions for Hyperconnectivity and the Internet of Things (pp. 130-150). IGI Global.

[47] Gupta, P., Kumar, V. and Yadav, V., 2021. Student's Perception towards Mobile learning using Interned Enabled Mobile devices during COVID-19. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 8(29), pp.e1-e1.

[48] Narayan, Vipul, et al. "A Comprehensive Review of Various Approach for Medical Image Segmentation and Disease Prediction.

[49] Mall, Pawan Kumar, et al. "A comprehensive review of deep neural networks for medical image processing: Recent developments and future opportunities." Healthcare Analytics (2023): 100216.

[50] Narayan, Vipul, et al. "Severity of Lumpy Disease detection based on Deep Learning Technique." 2023 International Conference on Disruptive Technologies (ICDT). IEEE, 2023.

[51] Saxena, Aditya, et al. "Comparative Analysis Of AI Regression And Classification Models For Predicting House Damages İn Nepal: Proposed Architectures And Techniques." Journal of Pharmaceutical Negative Results (2022): 6203-6215.

[52] 36. Kumar, Vaibhav, et al. "A Machine Learning Approach For Predicting Onset And Progression""Towards Early Detection Of Chronic Diseases "." Journal of Pharmaceutical Negative Results (2022): 6195-6202.

[53] 37. Chaturvedi, Pooja, A. K. Daniel, and Vipul Narayan. "A Novel Heuristic for Maximizing Lifetime of Target Coverage in Wireless Sensor Networks." Advanced

Wireless Communication and Sensor Networks. Chapman and Hall/CRC 227-242.

[54] Deshwal, V., Kumar, V., Shukla, R. and Yadav, V., 2022. Estimating COVID-19 Cases Using Machine Learning Regression Algorithms. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering), 15(5), pp.390-400

[55] Mr. Anish Dhabliya. (2013). Ultra Wide Band Pulse Generation Using Advanced Design System Software . International Journal of New Practices in Management and Engineering, 2(02), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/14

[56] Singh, M. ., Angurala, D. M. ., & Bala, D. M. . (2020). Bone Tumour detection Using Feature Extraction with Classification by Deep Learning Techniques. Research Journal of Computer Systems and Engineering, 1(1), 23–27. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/21