Journal of Mathematical Modeling
Vol. 13, No. 4, 2025, pp. 899-916. Research Article

JMM

A prototype model for image authentication, tamper localization and image restoration

Seyed Amir Hossein Tabatabaei[†*], **Matin Mirzaei**[†], **Sadegh Eskandari**[†], **Amirhossein Norouzi**[†]

[†]*Department of Computer Science, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran*

Email(s): amirhossein.tabatabaei@guilan.ac.ir, mtinmirzaei2002@gmail.com, eskandari@guilan.ac.ir, amirhn.workmail@gmail.com

Abstract. In this work, an algorithm and a tool for image authentication and restoration based on DCT coefficients, classic cryptography primitives, and blockchain are presented[1]. The proposed scheme can verify the authenticity of an image that has been subjected to malicious alteration, localize the modified regions, and restore the original image. However, just the malicious areas (column-wise) will be reconstructed and substituted while the intact parts (columns) are left as are to save unnecessary reconstruction costs. The tool is currently provided as a prototype serving as a web interface that is able to detect the possible maliciously altered columns of the received image precisely and to store the generated hash on a blockchain structure in almost real time. Experimental results together with the analysis of the scheme presenting the performance and security of the approach are provided which enhances the usability and trustworthiness of the scheme in further developments.

Keywords: Image authentication, security, blockchain, web-interface, prototype.
AMS Subject Classification 2010: 97R70, 94A08, 94A60.

1 Introduction

1.1 Background

The rapid development of information technology has made multimedia a cornerstone of modern existence. Fueled by the ubiquitous growth of Internet-of-Things (IoT) networks, the volume of digital images and videos has exploded due to their seamless creation and instant sharing. However, as the volume of image-based communication escalates, implementing stringent security protocols for data

*Corresponding author
Received: 23 March 2025 / Revised: 9 June 2025 / Accepted: 12 June 2025
DOI: 10.22124/jmm.2025.30185.2704

[1]Source code appears in https://github.com/capamir/image-authentication

transmission has become a critical priority. Inadequate safeguards and protection scenarios leave multimedia content vulnerable to multiple cyberattacks that undermine key security safeguards such as data accuracy, identity verification and privacy-protection, and call ownership rights into question. These vulnerabilities are increasingly being exploited for illicit purposes, such as financial fraud, invasive data harvesting and extortionist ransomware tactics.

Traditional or classic cryptography methods including solutions based on symmetric or public key cryptography are not well-suited for the efficient and direct processing of image data exemplars. Indeed the lack of robustness in the traditional cryptography systems causes such challenges. As a result, the need for improved security in digital image transmission has drawn considerable attention from researchers and industry alike [4]. There is a taxonomy of image authentication schemes which can be referred by [10, 20]. The building blocks of such schemes are based on classic cryptography, image processing and image descriptors or feature generation techniques. However, the structures of existing image authentication schemes are not limited to the aforementioned taxonomy.

Emerging recent technologies like blockchain and its intrinsic property like distributed trust and signature, bring the attention of domain experts to include such technology into their design. Introducing chaotic maps into image encryption is another approach in the area of image encryption and authentication which has attracted several researchers in the field [3, 5, 7, 16, 19]. Existence of distributed trust, anonymity and everlasting records makes the blockchain structure an efficient and secure technology which can be embedded in several novel resource sharing applications demanding security.

The verification of received image in the receiving party is a very crucial issue for establishing and sustaining trust between the sender and receiver parties. This authentication scenario at the ending of communication pipeline even can be equipped with other additive functions like image reconstruction fully or partially. This point strengthens the capability of the whole scheme significantly.

1.2 Related works

In the proposed scheme, the generated hash vector of image is stored in a blockchain structure. Utilizing blockchain to store image hash or signature in a decentralized way has emerged in many image authentication schemes in recent years to ensure the integrity and trustworthiness of digital media. Some important works are being explored in this section. As one of the earliest works presented in [6], the authors proposed a novel framework that synergistically combines digital watermarking with blockchain technology to address challenges in digital copyright management. In this work, a system in which digital watermarks are embedded into multimedia content to assert and verify ownership is presented. The utilized blockchain structure acts as a decentralized, immutable ledger for storing watermark metadata and copyright information to enhance the traceability and integrity of copyright records. The experimental results demonstrate that this integrated approach effectively maintains watermark robustness and offers a reliable means for digital copyright verification, providing a promising solution for the evolving needs of digital rights management. In another work presented in [8], the authors proposed stegochain, a novel decentralized framework that integrates blockchain technology with an advanced steganographic scheme for secure image communication. The framework leverages a robust steganographic method based on dilated Robert's edge detection. By dilating the edge image, the approach increases the number of edge pixels available for data embedding, thereby significantly enhancing the payload capacity compared to traditional LSB-based methods. After embedding the secret data into the cover image, the resulting stego-image is encrypted using a shared secret key. This encrypted image is then segmented

into chunks (frames), each accompanied by a digital signature. These transactions are broadcast across a decentralized blockchain network, where validating nodes (including miners) verify the authenticity of each frame through signature checks and cryptographic hashing. The blockchain's inherent immutability ensures that any tampering with the stego-image would necessitate re-mining of subsequent blocks, thereby providing robust protection against attacks. The key contributions of the paper include: (i) the development of a steganographic embedding scheme that exploits dilated Robert's edge detection to achieve a higher payload with acceptable visual distortion; (ii) the integration of this scheme with a blockchain-based framework to ensure data integrity, authenticity, and non-repudiation in a decentralized environment; (iii) the introduction of digital signature verification and an innovative reward mechanism (virtual points) for miners, enhancing trust and security in the network; and (iv) comprehensive simulation results demonstrating that the proposed method outperforms state-of-the-art techniques in terms of payload capacity and quality metrics such as PSNR and SSIM.

In another work presented in [17], the authors proposed an authentication scheme for authenticating the integrity of remote-sensing image data. The proposed work is based on blockchain and perceptual image hashing algorithm which aims at protecting the integrity of remote-sensing image data while storing or transforming. Besides designing a perceptual image hashing algorithm, a storage and transmission framework enabling the transmission of image hash value together with a prototype validating the usability of the scheme are presented in their work. The algorithm for calculating and generating the perceptual image hash from the image data computes the hash value in three steps including preprocessing step, perceptual image hashing extraction and final hashing. The extracted features are mainly based on the low-frequency components and logistic mapping of the image data. The storage and transmission framework is based on three steps including initialization, request and transmission wherein the final image hash value is secured through storing a blockchain structure. It must be noted that this scheme uses cryptographic encryption for securing the generated perceptual hash vector. The security of the scheme against acceptable and minor image modification through image test set has been shown. Also, the sensitivity of the algorithm against malicious modification in the image test set has experimentally been practiced. The proposed scheme in [17] enables tamper localization throughout a perceptual image hashing algorithm. However, restoration process at the localized level is not shown.

The scheme presented in [1], is designed for secure image sharing in multi-user environments. It integrates reversible data hiding (RDH) and encryption to ensure confidentiality, integrity, authentication, access control, and availability of digital images. The framework overcomes the limitations of traditional security methods by embedding user signatures into images, encrypting the images, and utilizing blockchain for verification and secure distribution. The framework stores encrypted images and their metadata in a blockchain network to prevent tampering and unauthorized access and uses cryptographic hashing to ensure image integrity and non-repudiation. The proposed RDH method allows embedding more secret data into images compared to existing techniques. The embedded data is fully recoverable, preserving both image quality and hidden data. A multi-level user access control model defines three user categories to ensure better usability and scalability of the scheme.

1.3 Similar works

There are some works wherein the introduced schemes utilize common building blocks like frequency sub-band coefficients in the process of hash generation stored in the blockchain structure. The work presented in [18] proposes a digital image copyright protection method integrating blockchain and zero

trust mechanisms, using grotto murals as a case study. The system leverages elliptic curve digital signature algorithm (ECDSA) for copyright owner verification and elliptic curve cryptography (ECC) for data encryption. It ensures secure data transmission, access control, and integrity verification as the called security services. The proposed scheme utilizes ECDSA to authenticate copyright owners and ensures data integrity through digital signatures. Also, it employs random encryption mode for secure transmission and access control. The generated image hash is stored in blockchain while using interplanetary file system (IPFS) for bulk data storage to reduce costs. In this scheme, smart contract is executed to facilitate secure copyright registration, verification, and transactions after chaotic image encryption. The proposed scheme supports tamper detection and whole image restoration throughout image decryption. The proposed hash generation scheme in [18] utilizes DCT coefficients to increase the robustness of the scheme as well.

In another important work given in [2] as the main inspiration for our work in algorithm design, a new image authentication and verification mechanism that is based on Merkle tree algorithms has been introduced. The root of the Merkle tree gives a trustworthy place to keep image qualities. In image verification, each image can be verified using the Merkle tree method to get the hash value of the Merkle tree node on the path. Also, the method uses IPFS. The proposed image authentication scheme, uses cryptographic hash function and traditional encryption algorithm to detect and localize the modified regions of the image and restore the damaged parts at image block level. According to the results shown the proposed hashing scheme does not reduce the visual quality of the restored images significantly based on some image fidelity. The main difference between this work and ours, is utilizing DCT transformation instead of embedding operation in order to introduce some robustness into our scheme differently on each channel of the colorful image. Also in our work localization and restoration procedure is provided locally at the column level (throughout calculating the column hash and encryption) instead of the block level hash generation to save the cost. There exist some previous works in the literature which provide tamper localization and correction (partial image restoration) on grayscale images using low-frequency coefficients and error correcting codes as well [11, 12, 14]. Table 1 compares some functional properties among four similarly relevant image authentication schemes as follows.

Table 1: Comparison among similar schemes according to their base functionality

Scheme	Main use-case	Temper localization granularity	Localized image restoration
[17]	Remote-sensing imagery authentication	Block-level	(whole image restoration)
[18]	Copyright protection	–	–
[2]	Image authentication	Block-level	Yes
Ours	Image authentication	Column-level	Yes

1.4 Contribution of this work

In this work, a robust image authentication tool prototype ensuring the integrity verification, modification and altering localization and restoration on color images is developed. As the main contribution, the presented scheme is deployed as a web interface to be utilized for both grayscale and colorful image authentication, restoration and verification. This verification is crucial for establishing trust between the

communication parties. The proposed model is also suitable for applications wherein the image hash is stored in a blockchain structure and the smart contracts are being involved and the quality preservation of the restored images is of high importance. However in this work just the storage on the blockchain structure is proposed. Consequently, the source of each image becomes transparent and traceable, significantly enhancing the security of the entire communication system. Finally, to adjust the usability of the scheme based on the use-case and application, important security analysis of the scheme has been provided as well.

The rest of this paper is as follows. The scheme for image authentication and restoration together with the algorithms specification is presented in Section 2. The deployed tool prototype as a web interface is presented in Section 3. Section 4 presents the experimental results to validate the claimed features of the scheme empirically. Security consideration is described in Section 5. Section 6 concludes the paper.

2 Image authentication and restoration based on low-frequency coefficients and cryptography

2.1 General model and used technologies

The proposed image authentication scheme utilizes DCT for the sake of transferring image to the frequency space in hash generation phase. Applying column-based cryptography hashing as well as encryption enables malicious or altering region(s) detection. The verification phase utilizes blockchain structure to securely distributes the signature across the network. The detailed structures of both hash generation phase as well as hash verification phase come as follows.

2.2 Hash generation

2.2.1 Hash generation of grayscale images

The hash generation phase consists of three main steps including transformation, column-based hash computation/encryption and final hash producing. In the transformation step, the DCT is applied on the image after dividing the image into non-overlapping blocks in a block-wise manner. However, only partial coefficients will be kept for hash calculation. In the second step, a cryptographic encryption algorithm as well as hashing algorithm is used to encrypt and hash stored partial DCT coefficients. In the third step, a block containing the image meta-data as well hash words is shaped. This block is attached to the utilized blockchain structure. The details of the image hash generation phase is described as follows in Algorithm 1.

2.2.2 Hash generation of color images

The aforementioned image authentication scheme is extended to color images as well. In this case, at first the image is decomposed into three channels (Y, Cb, Cr) and then the DCT is applied on each channel. However to reduce the computational cost significantly, the DCT is performed just on Y channel block-wise and the other channels will be subjected to the DCT as whole. Indeed the process of generating image hash vector on the Y channel is exactly the same as Algorithm 1 above. The encryption operation on channels Cb and Cr are also light in comparison with grayscale images and consists of encrypting the

Algorithm 1 Hash generation algorithm

1: **Input:** Image I of size $n \times m$, number of blocks k^2, ratio of DCT coefficients r_{DCT}, secret key k
2: **Output:** Image hash vector H
3: Divide image I into k^2 non-overlapping blocks $I_1, ..., I_{k^2}$
4: Calculate 2d-DCT on each block: $B_i = 2d - DCT(I_i), i = 1, ..., k^2$
5: Shape DCT matrix $[DCT]_{k,k}$ by keeping r_{DCT} of DCT coefficients of each block B_i
6: Column-based encryption on $[DCT]_{i,j}$: $E = ENC_k([DCT]_{i,j} = (E_1, ..., E_k))$
7: Column-based hashing on $[DCT]_{i,j}$: $h = HASH([DCT]_{k,k} = (h_1, ..., h_k))$
8: **Return** final hash value as $H = E||h$

selected coefficients of the DCT of whole image block. Also, the cryptographic hash on channels Cb and Cr is not computed to reduce the computational load even more. Therefore, the final hash vector of image $I = (Y, Cb, Cr)$ is as follows:

$$Hash(I) = H(Y)||Enc\{DCT - Cb_{\{i_1,...,i_p\}}\}||Enc\{DCT - Cr_{\{i_1,...,i_p\}}\}, \quad (1)$$

wherein the indexes $i_1, \ldots, i_p$ indicate the selected coefficients of DCT matrix.

Length of the generated hash of the input image is not fixed and depends on the image size and the input parameter r_{DCT}. The choices for utilized cryptographic hashing and encryption algorithms are also depending on the users preferences. Typical algorithms are AES and SHA-256 for encrypting and hashing, respectively. Further security enhancement can be obtained by using message authentication codes (MAC) instead of traditional hashing algorithm in Algorithm 1.

2.3 Hash verification and partial image restoration

2.3.1 Hash verification and partial image restoration of grayscale images

The process of hash verification consists of possible error detection, localization and partial image restoration. The receiver computes the hash of the image upon receiving and compares it with the received hash sequence column-wise. The mismatched words indicate the erroneous columns (or forged columns). To reconstruct the erroneous or forged column(s), the marked encrypted word(s) are decrypted and the column(s) are reconstructed using an inverse transform of the 2d-DCT. Details of the hash verification and partial image reconstruction is as follows in Algorithm 2.

Although the proposed scheme allows for partial reconstruction of the image, it is important to note that the quality of the reconstructed image will likely be inferior to the original image. This degradation occurs since the reconstruction relies solely on a portion of the retained DCT coefficients, which capture most of the image's energy, rather than preserving the complete energy content.

2.3.2 Hash verification and partial image restoration of color images

The general process of hash verification is trivially the same as grayscale images, however the reconstruction process is partially different. In fact, when a color image is subjected to integrity verification, if the verification on Y channel is being succeeded then the image is verified as authentic. However, if the verification fails on Y channel then reconstruction process is performed using recovered tamper columns

Algorithm 2 Hash verification and partial image reconstruction

1: **Input:** Received image $I\prime$, received image hash $H\prime$, secret key k
2: **Output:**1 (if the image is verified as original), reconstructed image I" (if the image is verified as erroneous)
3: Calculate hash of the received image $I\prime$ according to the hash generation algorithm 1 and denote it by $H" = E"||h"$
4: **IF** $H" == H\prime$ return 1
5: **ENDIF**
6: Mark detected erroneous column(s) by indexes set $EC = \{i_1, ..., i_m\}$
7: Recover the DCT coefficients by decryption of columns indexed by the set EC: $DC = Dec(I\prime_{EC}) = \{J_{i_1}, ..., J_{i_m}\}$
8: Apply inverse of 2d-DCT on DC: $2d - DCT^{-1}(DC) = \{J_{I"_1}, ..., I"_{i_m}\}$
9: Substitute the columns indexed by EC with $\{J_{I"_1}, ..., I"_{i_m}\}$ in image $I\prime$
10: **Return** $I\prime$

of Y image combining with the recovered Cb and Cr images. It is worth mentioning that the restored image wherein the detected tampered area(s) is partially reconstructed is being subjected to distortion (only in the detected tampered locations) due to the limited stored coefficients. However, this issue can be avoided by increasing the memory cost when the application is sensitive and retaining more DCT coefficients.

2.4 Storing and distributing the image hash

Generated hash vector of the image is secured and further stored as a content of a block into a block chain structure. The advantage of usage of image hash is to publish the final hash vector of the final hash of the image in a distributed form in order to avoid possible active attacks. Each block in the blockchain is designed to store specific types of data, ensuring the system functionality, security, and integrity:

1. Index field: an integer which represents the position of the block in the blockchain, starting with 0 for the genesis block and incrementing by 1 for each subsequent block.

2. Timestamp field: a DateTime value, which records the exact time when the block was created, providing a chronological record of when the image data was processed and stored.

3. Previous hash field: a string, which stores the hash of the previous block, ensuring the immutability of the blockchain by linking blocks together.

4. Hash field: a string which stores the partial hash words of the image including just column-wise hash words generated according to Algorithm 1.

In order to retrieve the image information for the sake of image restoration, the encrypted image information according to Algorithm 1 has to be stored. However, tamper localization takes place according to the image hash reference while the encrypted file is not stored in the blockchain due to its size. In fact, image retrieval takes place based on off-chain storage with an on-chain reference wherein the reference to the corresponding encrypted file is stored in the blockchain. The decentralized storage

options suitable for storing the encrypted image files include IFPS (like [2]), Swarm (like [17]), Arweave or Sia for example. The mechanism for sharing the key of symmetric encryption algorithm employs asymmetric encryption to securely upload the encrypted key (to be used for symmetric encryption) in the corresponding block of the on-chain structure. Overall pipeline of the hash generation, storing and verification is depicted in the following figure.

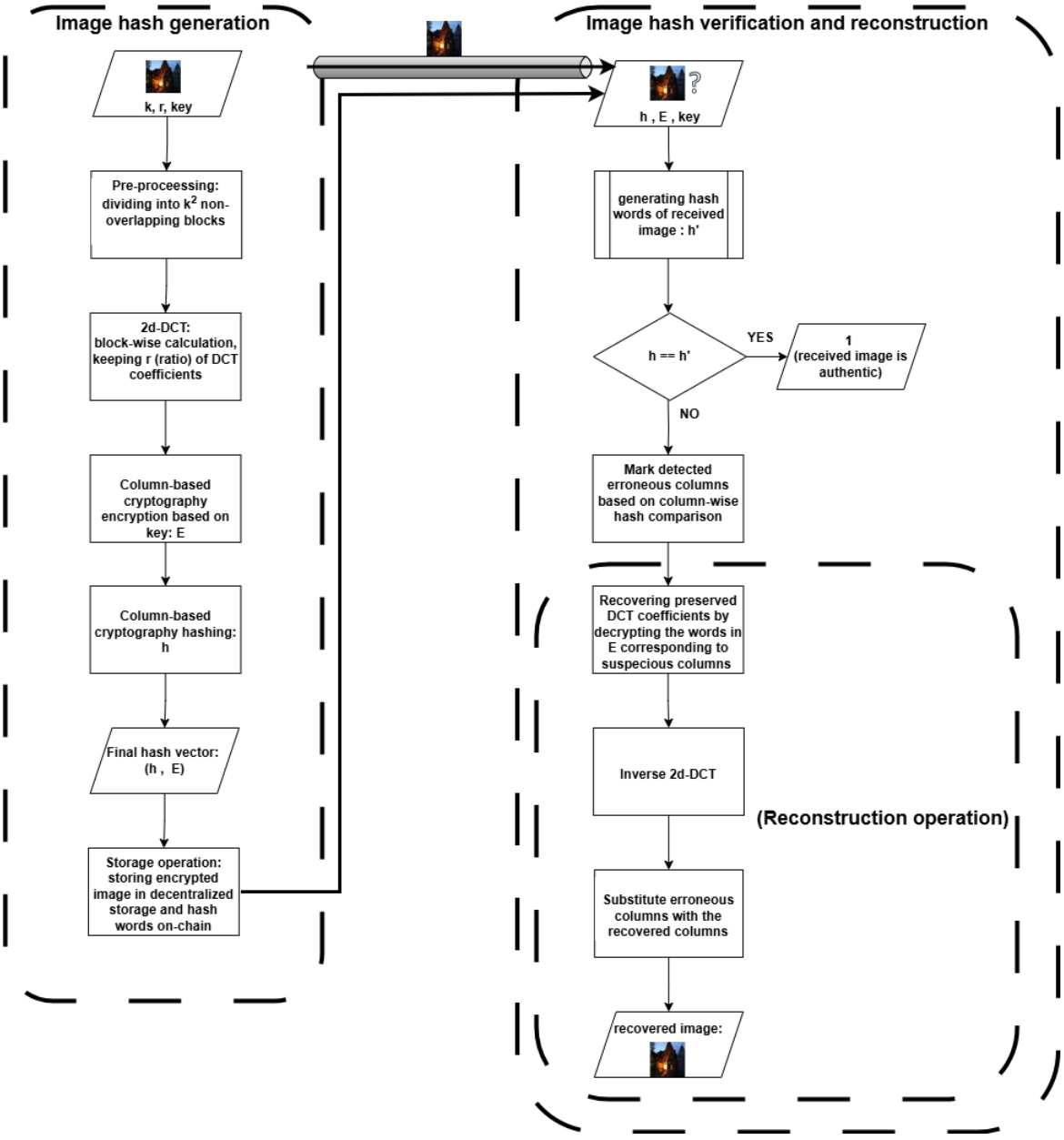

Figure 1: Overall pipeline of the hash generation, storing and verification/restoration

3 Image authentication tool as a web interface

3.1 Introduced tool

The aforementioned image authentication and restoration scheme is deployed as a web interface. The introduced tool currently is at the prototype level which enables all functionality defined by the scheme including authentication, altering localization, and image restoration. The tool prototype is a sophisticated solution designed for image authentication and verification, ensuring data integrity and security through a series of advanced image processing and cryptographic techniques. The tool operates two main features of the scheme: image hash generation and image verification and possible restoration. The restoration operation is performed partially only on the detected localized parts wherein the alteration is detected at the column level to save the computational cost. These functionalities are shown in Figure 2.

3.2 Implementation technology

The back-end has been implemented by Django while the front-end by React.js. The implemented back-end powered by Django REST Framework (DRF) provides a robust API to handle all features defined in the scheme including image processing, encryption and blockchain integration. Its scalability and security features make it an ideal choice for managing defined complex operations in our proposed scheme. At the front side, React.js provides a dynamic and user-friendly interface with React Router DOM enabling seamless navigation and smooth communication between front and back sides. This combination ensures a responsive and intuitive user experience while maintaining the platform reliable and efficient. Also, the blockchain structure is built using Django ORM to define models like block, referring it and retrieving the information. Model architecture of the developed interface as depicted as follows in Figure 3. The implementation was performed on a laptop with an AMD Ryzen 5 5500U and integrated AMD Radeon Graphics with 16 GB RAM running Windows 11 Pro. The authentication time (hash generation and on-chain storage) with retaining ratios of 0.05, 0.15, 0.25 and image resolution of 128 x 128 (1024 x 683) is 6.02, 6.14, and 6.17 (6.77, 7.33, and 7.53) seconds while the corresponding verification times are 0.03, 0.06, and 0.09 (0.33, 0.62, and 0.84) second, respectively.

4 Experimental results and performance of the scheme

4.1 Sensitivity of the scheme

The proposed image hashing scheme has been subjected to some test images from well-known datasets. The first dataset[1] contains original images as well as corresponding tampered images including copy, cut and trim modifications. The second dataset contains some benchmark images like Lena and Cameraman commonly used as test images. The original images are either grayscale or colorful images which are converted to grayscale ones using Otsu's threshold method. The proposed image hashing algorithm has been used to generate the hash of both original and corresponding tampered images and the verification algorithm is utilized to detect the tampered areas (columns) and reconstruction. The results are shown as follows (Figure 4).

[1] https://www5.cs.fau.de/resear/-ch/data/image-manipulation/index.html

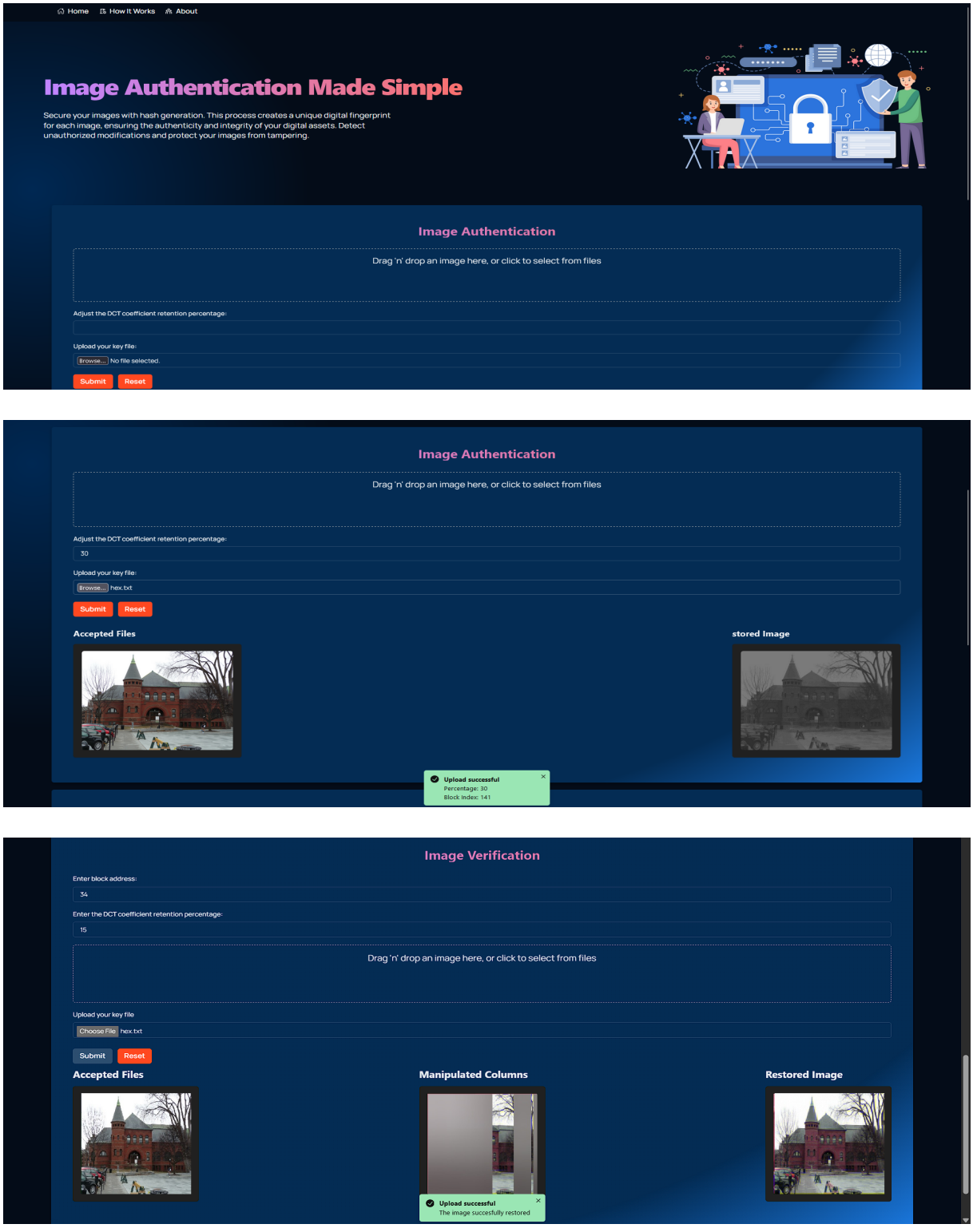

Figure 2: Developed tool for image authentication, verification and restoration, from top to bottom: start page (hash generation), image verification, initial results, restored image

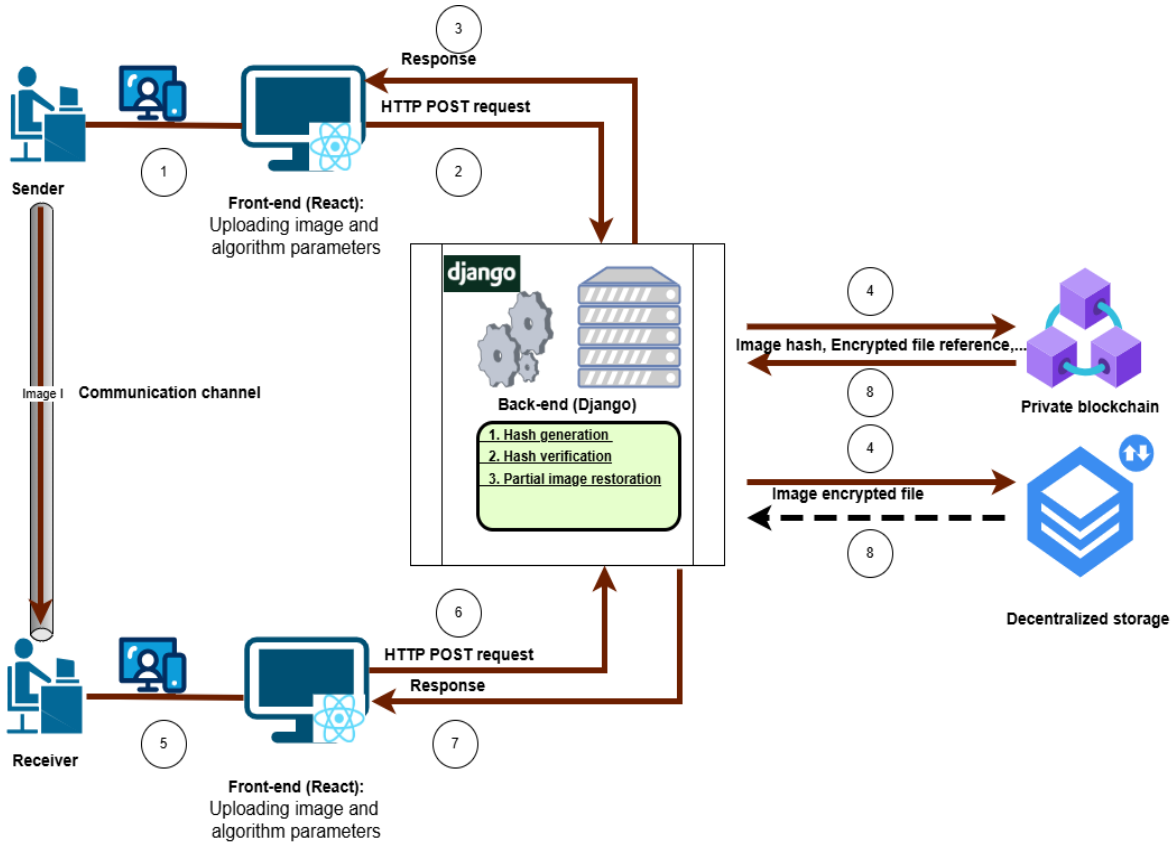

Figure 3: Pipeline of the usage of prototype of image authentication, verification and restoration scheme

As expected, the reconstructed areas have been degraded in terms of visual qualification due to keeping only low-frequency components of DCT matrix in the reconstruction process. The image hash size can be sacrificed at the cost of increasing the reconstruction quality in image restoration process. Similar test has been performed on color images according to the algorithm presented in Subsection 2.3.2. The corresponding results wherein the manipulated images are restored in a form of original color images. The results are shown as follows in Figure 5.

4.2 Evaluating visual quality of restored images

To quantify the qualification capability of the reconstructed images, it is a common practice to use image quality measures. peak of signal to noise ratio (PSNR) is one of the commonly used measures as an indicator which implies to representation fidelity. This measure is not an absolute measure and the usage makes sense when a comparison is being made. Besides, the PSNR is a poor metric in comparison with other metrics. So, two other metrics as information fidelity criterion (IFC) and visual information fidelity (VIF) have been computed for the test case images (original image I and noisy image $I\prime$). The two latter metrics have been shown to have a better performance in approximating the visual quality judgments [15]. In fact, the IFC is more a fidelity criterion than a distortion metric. The descriptions of

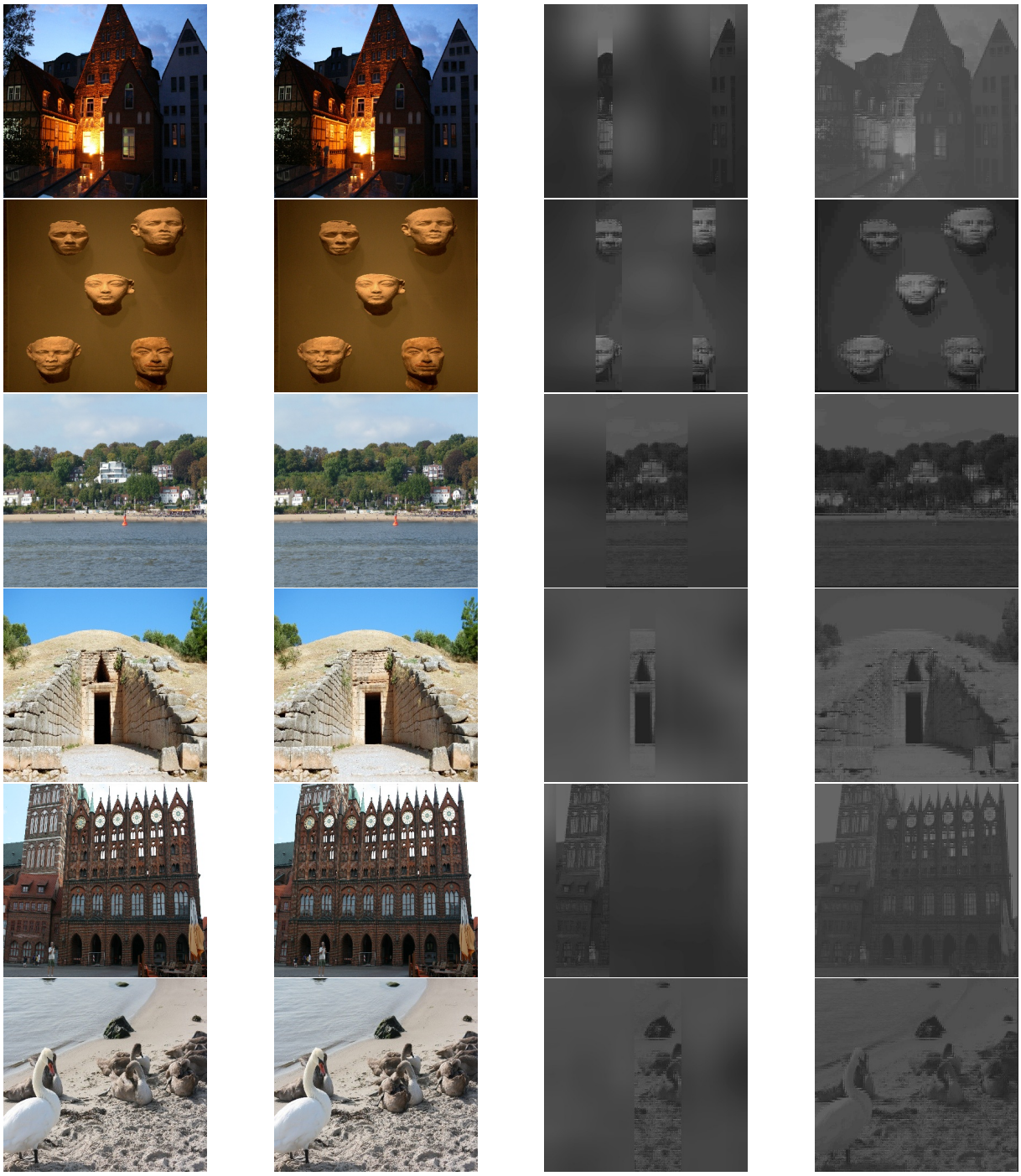

Figure 4: Detection and restoring the images subjected to malicious modification from left to right: original images, forged images, images whose modified columns are detected, restored images

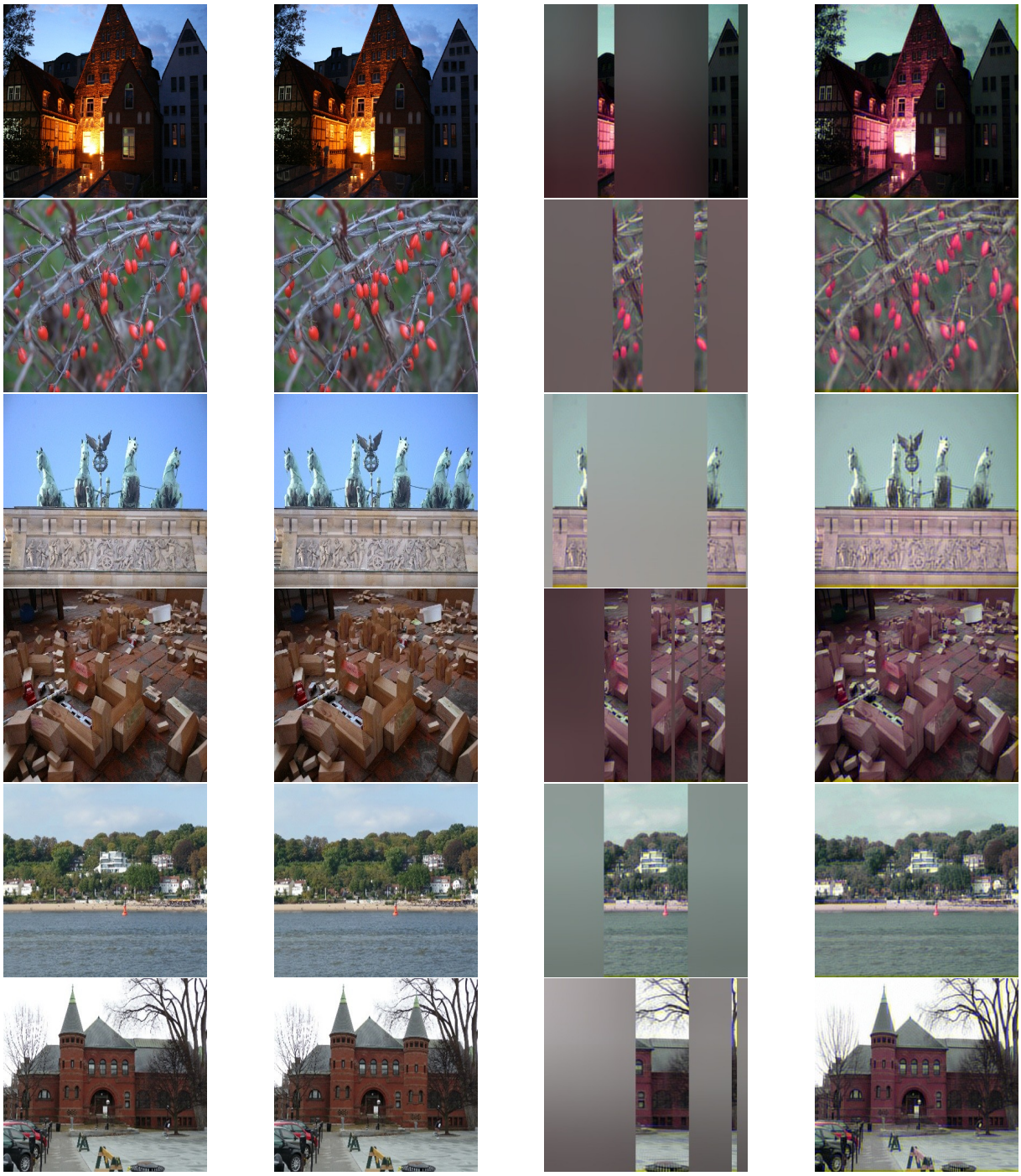

Figure 5: Detection and restoring the color images subjected to malicious modification from left to right: original images, forged images, images whose modified columns are detected, restored images

the utilized three metrics are as follows:

1. PSNR:

$$PSNR = 10\log_{10}(\frac{MAX_I^2}{MSE}), \tag{2}$$
$$MSE = \frac{1}{mn}\Sigma_{i=0}^{m-1}\Sigma_{j=0}^{n-1}(I(i,j) - I\prime(i,j))^2$$

   In the above formula, MAX_I is the maximum pixel value (depending on the pixel depth) and, $I(i,j)$ and $I\prime(i,j)$ represent the pixel value at location (i,j) corresponding to noisy and original image respectively.

2. IFC:

$$IFC = \Sigma_{i\in subbands} I(C^{N_i,k}, D^{N_i,k}|S^{N_i,k}), \tag{3}$$

   where, I is mutual information function and $C^{N_i,k}$ denotes the N_k coefficients from the wavelet coefficients of the reference (original) image I in the k subband, and $D^{N_i,k}$ is defined as the corresponding coefficients in the distorted (noisy) image. Finally $S^{N_i,k}$ indicates the same coefficients (as defined for $C^{N_i,k}$ and $D^{N_i,k}$) corresponding to the scaling field in the Gaussian scale mixture (GSM) model. The details are presented in [9]. VIF assesses the amount of visual information preserved in a restored image relative to the reference (original) image and computed as follows:

3. VIF:

$$VIF = \frac{\Sigma_{i\in subbands} I(C^{N_i,k}, F^{N_i,k}\|S^{N_i,k})}{\Sigma_{i\in subbands} I(C^{N_i,k}, E^{N_i,k}\|S^{N_i,k})}, \tag{4}$$

   where, $F^{N_i,k}$ denotes the N_k coefficients from the wavelet coefficients of the restored image in the k subband after human visual system (HSV) noise, and similarly, $E^{N_i,k}$ is defined for the reference image.

In fact, the latter two image fidelity criteria both are based on information-theoretic concepts and measures the amount of information preserved in a restored image. Specially, estimating the HVS parameters is crucial for the VIF index, as they model the perceptual characteristics of human vision. The aforementioned image fidelity measures have been calculated for the test images as shown in Figure 6. According to the plot, the image quality of the restored images from perceptual viewpoint is preserved in a reasonable range which empowers the usability of the proposed scheme in several applications in which the noise resources are present. It must be noted that the visual quality of recovered images is highly depending on the ratio of recovered DCT coefficients which is specified based on the requirements and use-cases. In fact, the memory and computational cost concerns play an important role in assigning the value to this ratio.

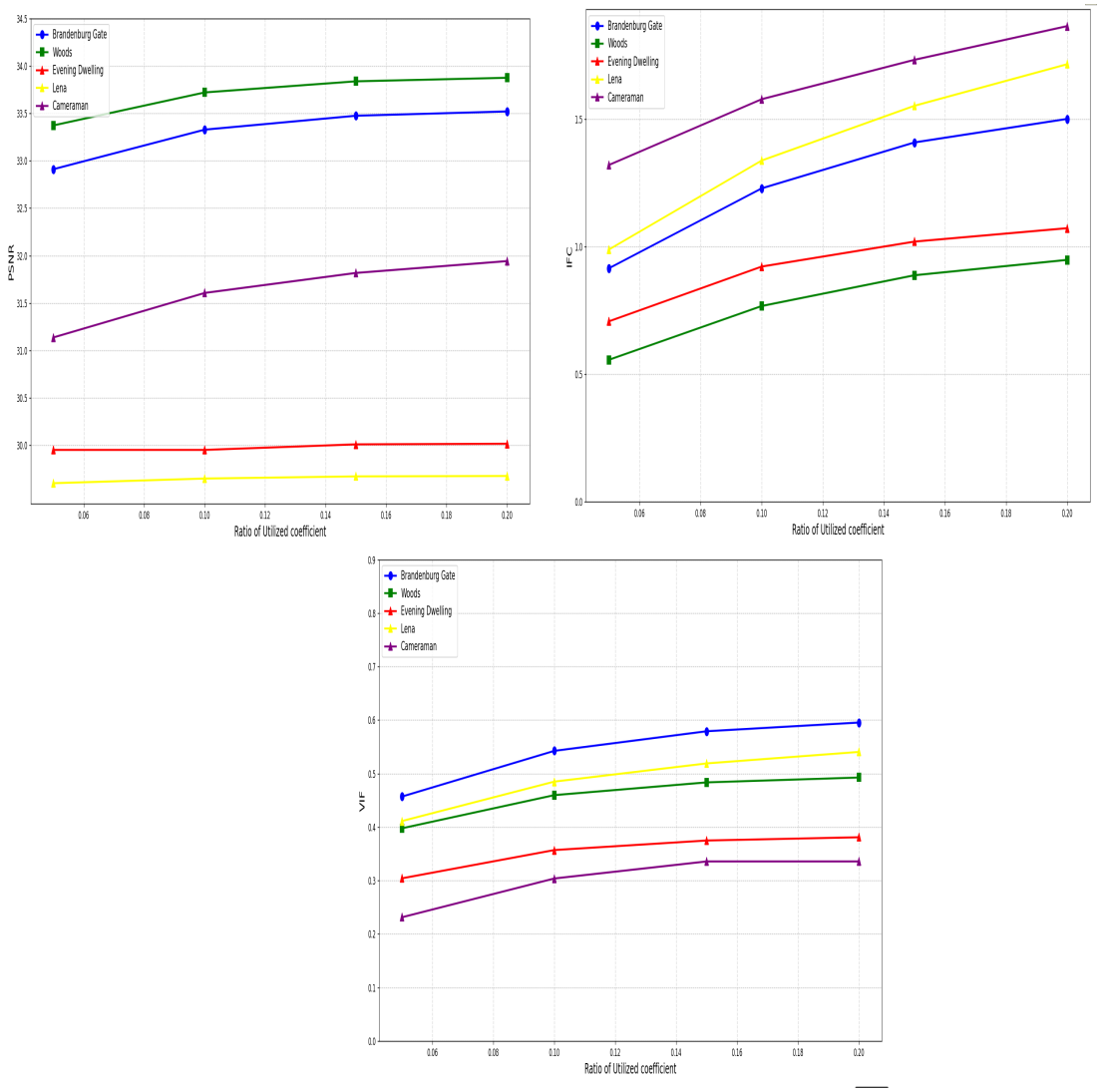

Figure 6: Image fidelity criteria of test images presented as PSNR, IFC, and VIF measures

5 Security of the scheme

When considering an image authentication scheme, two types of attack scenarios are considered: active and passive types. In an active attack scenario, the attacker tries to involve actively in altering, manipulating or injecting the data flowing in the system. The active attack on the primitive itself includes tampering attack in which the attacker tries to modify an authenticated image and generate the corresponding hash to deceive the receiver in accepting the new image-hash pair. One prominent example of such attacks on image authentication schemes is the collage attack wherein the attacker tries to create a forged image by combining some parts from other different images. To successfully launch this attack, the attacker must substitute the hash word of corresponding column which is secured via blockchain. In fact, the required complexity of a successful attack is equivalent to creating a collision for a block to compromise the

blockchain intrinsic security. This attack can be also primitively hindered either by adding an encryption operation after generating the column-based hashes or by generating the column-wise MAC instead of traditional hashing algorithm to diffuse the generated hash words before on-chain storing. Another important example of an active attack is a brute-force hash substitution attack wherein the attacker tries to recover the original image or parts of it by trying all possible hash-function-generated keys. Using strong hash function and longer key remove vulnerability of the scheme against brute-force hash substitution attack. In a passive attack scenario, the attacker tries to monitor or eavesdrop on the system without actively altering the data. In this case for example, the attacker listens to the communication channel and tries to capture an image-hash and substitute it with another valid image-hash pair.

To analyze the scheme, let Tr_{acc} be the acceptance threshold value set for the difference between the hashes of original image and the received one submitted at the receiver side. Similarly, let T_a be the acceptance threshold value (in terms of image blocks) set for differences between the original image and the received one for a successful verification. Here, we calculate two important probabilities which are applied in analyzing the security in aforementioned scenarios [13]. The first probability, P_1, indicates the probability of accepting a received image whose difference with the one from the reference image is less than predefined threshold T_a blocks. We expect to have $P_1 \to 1$ ideally. To calculate P_1, let I and $I\prime$ be two images and H and $H\prime$ be their corresponding final hash values. Also suppose that N be the length of final hash value and m and n denote the number of columns and rows, respectively. To calculate P_1, we must calculate the probability of possible cases in which the hash values have maximum Tr_{acc} differences from each other. P_1 is calculated as follows:

$$P_1 = \sum_{i=0}^{Tr_{acc}} \binom{Tr_{acc}}{i} \Big(\sum_{j=0}^{\min(n,T_a)} \binom{n}{j} \Big(\frac{1}{nm}\Big)^j \times \Big(1-\frac{1}{nm}\Big)^{(n-j)i} \Big(1 - \sum_{j=0}^{\min(n,T_a)} \binom{n}{j} \Big(\frac{1}{nm}\Big)^j \Big(1-\frac{1}{nm}\Big)^{n-j}\Big)^{Tr_{acc}-i}. \tag{5}$$

The other probability is called P_2 and realizes a lower bound for the chance of rejecting a non-authentic received image with d number of different blocks which $d > T_a$. This probability is calculated based on a similar probability model as P_1 as follows:

$$P_2 = \sum_{i=Tr_{acc}}^{m} \binom{Tr_{acc}}{i} \Big(\sum_{j=\min(n,T_a)}^{n} \binom{n}{j} \Big(\frac{1}{nm}\Big)^j \times \Big(1-\frac{1}{nm}\Big)^{(n-j)i} \Big(1 - \sum_{j=\min(n,T_a)}^{n} \binom{n}{j} \Big(\frac{1}{nm}\Big)^j \Big(1-\frac{1}{nm}\Big)^{n-j}\Big)^{Tr_{acc}-i}. \tag{6}$$

The calculation of P_1 and P_2 is based on the requirement analysis of the application wherein the proposed image authentication scheme is embedded in it. The user can adjust the robustness and sensitivity of the scheme by customizing the parameters P_1 and P_2 based on predefined lower and upper thresholds Tr_{acc} and T_a, number of blocks m and n and quantization factor.

As the image tags are created from cryptographic primitives and stored in a blockchain structure, the data integrity verification throughout the chain, resistance against unauthorized access, and tamper/fraud proof are inherited directly to the scheme.

6 Concluding remarks

In this paper, a web-based interface as a tool prototype for robust image authentication, verification and restoration scheme based on the DCT, classical authentication and integrity solutions, and blockchain has been introduced. The presented scheme, is able to provide the authenticity of the image subjected to some malicious or acceptable modification based on some threshold values to be adjusted by the user. The security of the scheme is either inherited from the security of the cryptography algorithm or based on blockchain. However, as a scheme is equipped with a soft authentication scenario based on the thresholds, the corresponding probabilities have been computed. Quality of the reconstructed images have been compared with the original images with reference to three different metric types. Our future follow up work is concentrated on industrializing the scheme (promoting the technology readiness level) and implementing on a public or private blockchain structure. Also promoting the usability of the scheme through enabling batch of images (with flexible sizes) processing and providing integration support for developers will be considered as the next development phase.

References

[1] D. Brabin, C. Ananth, S. Bojjagani, *Blockchain based security framework for sharing digital images using reversible data hiding and encryption*, Multimed. Tools Appl. **81** (2022) 24721–24738.

[2] Y. Chen, Y. Chou, Y. Chou, *An image authentication scheme using Merkle tree mechanisms*, Future Internet **11** (2019) 149.

[3] L. Gong, H. Luo, R. Wu, N. Zhou, *New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG*, Physica A **591** (2022) 126793.

[4] Z. Guo, S. Chen, L. Zhou, L. Gong, *Optical image encryption and authentication scheme with computational ghost imaging*, Appl. Math. Model. **131** (2024) 49–66.

[5] Q. Liang, C. Zhu, *A new one-dimensional chaotic map for image encryption scheme based on random DNA coding*, Opt. Laser Technol. **160** (2023) 109033.

[6] Z. Meng, T. Morizumi, S. Miyata, H. Kinoshita, *Design scheme of copyright management system based on digital watermarking and blockchain*, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 2018, 359–364.

[7] Y. Sang, J. Sang, M. Alam, *Image encryption based on logistic chaotic systems and deep autoencoder*, Pattern Recogn. Lett. **153** (2022) 59–66.

[8] P. Sarkar, S. Ghosal, M. Sarkar, *Stego-chain: A framework to mine encoded stego-block in a decentralized network*, J. King Saud Univ. Comput. Inf. Sci. **34** (2022) 5349–5365.

[9] H. Sheikh, A. Bovik, G. de Veciana, *An information fidelity criterion for image quality assessment using natural scene statistics*, IEEE Trans. Image Process. **14** (2005) 2117–2128.

[10] S. Tabatabaei, N. Živić, *A review of approximate message authentication codes*, in: N. Živić (Ed.), *Robust Image Authentication in the Presence of Noise*, Springer International Publishing, 2015, 105–127.

[11] S. Tabatabaei, O. Ur-Rehman, N. Živić, C. Ruland, *Secure and robust two-phase image authentication*, IEEE Trans. Multimed. **17** (2015) 945–956.

[12] S. Tabatabaei, O. Ur-Rehman, N. Živić, *AACI: The mechanism for approximate authentication and correction of images*, in: 2013 IEEE International Conference on Communications Workshops (ICC), 2013, 717–722.

[13] D. Tonien, R. Safavi-Naini, P. Nickolas, *Breaking and repairing an approximate message authentication scheme*, Discrete Math. Algorithms Appl. **3** (2011) 393–412.

[14] O. Ur-Rehman, S. Tabatabaei, N. Živić, C. Ruland, *Soft authentication and correction of images*, in: SCC 2013; 9th International ITG Conference on Systems, Communication and Coding, 2013, 1-6.

[15] R. Wajid, A. Mansoor, M. Pedersen, *A human perception based performance evaluation of image quality metrics*, in: International Symposium on Visual Computing, 2014.

[16] X. Wang, N. Guan, J. Yang, *Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map*, Chaos Solitons Fractals **150** (2021) 111117.

[17] D. Xu, N. Ren, C. Zhu, *Integrity authentication based on blockchain and perceptual hash for remote-sensing imagery*, Remote Sens. **15** (2023) 4860.

[18] Q. Zhang, G. Wu, R. Yang, J. Chen, *Digital image copyright protection method based on blockchain and zero trust mechanism*, Multimed. Tools Appl. **83** (2024) 77267–77302.

[19] N. Zhou, L. Hu, Z. Huang, M. Wang, G. Luo, *Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm*, Expert Syst. Appl. **238** (2024) 122052.

[20] N. Živić (Ed.), *Robust Image Authentication in the Presence of Noise*, Springer International Publishing AG, 2015.