International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A VISUAL CRYPTOGRAPHY WATERMARKING SYSTEM FOR DETECTING AND IDENTIFYING TAMPERED IMAGES

K.GAYATHRI NAGA BHANU
ECE
INSTITUTE OF AERONAUTICAL ENGINEERING
HYDERABAD
21951a0453@iare.ac.in

N.HARINI
ECE
INSTITUTE OF AERONAUTICAL ENGINEERING
HYDERABAD
21951a0458@iare.ac.in

G.DINEETH UDBHAV
ECE
INSTITUTE OF AERONAUTICAL ENGINEERING
HYDERABAD
21951a0448@iare.ac.in

MR.V.PRASANNANJANEYA REDDY
ECE
INSTITUTE OF AERONAUTICAL ENGINEERING
HYDERABAD
Prasanna.vajrala@gmail.com

Abstract: ***In the current digital era, protecting the legitimation and integrity of the image is of the main problems due to the wide access of image editing tools for forgeries. This report presents a watermarking approach based on visual cryptography for the detection and localization of image forgery. The suggestion deals with putting a watermark on the host image by visual cryptography. This was the division of the image into several parts. However, only when all these shares are placed on top of each other at the correct position the watermark is visible. As a result, the watermark is hidden, the secrecy is preserved, and the security of the watermark improves. With the use of cryptographic shares within the watermark, the technique enables detection and restitution of a point of the image that the tamper has altered. Visual cryptography is used to ensure that the watermark is invisible and, it is a security artwork that protects the watermark against unauthorized extraction. The data along with the experimental results are conveyed demonstrating that the method withstands regular image processing operations and is quite good at alteration detection while maintaining image quality. This method is very useful in the scope of image forensic studies, copyright and input verification.***

Keywords: ***Visual cryptography, watermarking, image forgery detection, image forgery localization, cryptographic shares, digital forensics, content authentication, copyright protection, image integrity, tamper detection, invisible watermarking, robust watermarking.***

I. INTRODUCTION

Visual Cryptography (VC) is a simple form of the visual concept of cryptography which was developed by Naor, and Shamir in 1994 known as VSS. Altogether, Basic VC is characteristically used when transferring photographs, hand writings, financial statements, textbook images, topological maps used in military operations, satellite communications etc It is the process of dividing the Secret image into shares so that enough shares next to each other reveal the Secret image. Shares originally means binary images of the secret image. This can be decrypted by placing all the shares on top of one another and a human would be able to distinguish the secret picture lying in this stack as the human visual system does. The simplest way to do that is to print it on one layer to a transparent sheet two times.

Visual cryptography is a system that an image is divided into many sections and, no section reveals any information at all. This means that when these shares are placed one over the other, that is, superimposed then the concealed image will be revealed. It does not involve some Mathematical operations, rather, it mainly involves simple two-fold operations. The other way through which people protect their owned contents such as images and videos to regain their ownership and protect their copyrights is called digital watermarking. It is therefore clear that a good watermark should be invisible to human perception and also be resistant to the different types of attacks and manipulations. Visual cryptography, which is a part of a visual cryptography-based watermarking, is a blend of visual cryptography with digital watermarking. In other words, using this method, principles of visual cryptography are used to embed watermark information within digital pictures to reveal some hidden watermark only under certain circumstances. It is a formidable method of protecting digital content but it presents the problem of storage, transmission and image quality in as careful a manner as possible.

Image forgery detection has become more significant in this modern age of information technology for a variety of reasons:

Image forgery detection has become more significant in this modern age of information

technology for a variety of reasons:

1. Security and Authentication
2. Trust and Credibility
3. Legal and Ethical
4. Economic Impact

PROBLEM STATEMENT

The advancement in the use of digital image in various fields such as media and entertainment, medical diagnosis, and even in legal processes have required the use of authentication in images. Photomontage, which may be described as the act of altering images without permission from the owner, is still a major threat to the authenticity of digital visual content. Traditional techniques of securing image data depend on mathematical algorithms and it is difficult for the final consumer to determine reliability or authenticity of the data. It also makes it convenient for the world to have stable, secure, and efficient means of detecting and removing image manipulation. Some of the currently used methods of watermarking are; Current watermarking has the following drawbacks; This could be the case with the visual cryptography which has the tendency of becoming a very efficient tool but the prospects of its application in the watermarking for forgery detection and localization has to undergo much more active research.

II. RELATED WORK

Over the years, several algorithms have been developed in detecting image forgeries and watermarking these images, starting with spatial domain and proceeding to frequency domain. Conventional methods including DCT and DWT have been applied for watermarking images in order to detect tampering or to prevent copying of images. However, these methods have some problems when it is trade-off between stealth and anti-attack capability. There are new developments in cryptography known as visual cryptography schemes where an image is split into share that can only be viewed overlaid. Conjunctional techniques of cryptography and watermarking for instance Chaotic encryption-based watermarking can be very effective in providing higher degree of security and anti- tamper characteristics. However, some issues are still open; namely, how to localize the tampered regions adequately and keep the watermark both invisible and visually pleasant. The above methods are utilized in the proposed approach; however, the watermarking is combined with the use of visual cryptography; Providing enhanced capabilities in detecting and localizing image forgeries without compromising the quality of the watermark, which is designed to be invisible during routine usage.

A. Conventional methods: DCT and DWT

In watermarking to detect forgery, two techniques are commonly used and these are Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). According to the way DCT works, it maps an image from the spatial domain to the frequency domain where the watermark data is inserted on the less visible high frequency parts of the signal to make the watermark resistant to attacks such as compression. On the other hand, DWT breaks down the image into multiple frequency sub-bands for the water mark to be embedded in the particular sub-bands so that the water mark can be both, invisible and robust against any signal manipulation or attempts at forgery. They improve the security and quality of digital content through embedding and extraction of watermarks for the identification of any changes or fakes.

B. Chaotic encryption-based watermarking

Chaotic encryption-based watermarking utilizes the propriety and delicate characteristic of the chaotic system for improving the security barriers in watermarking techniques. This approach involved the selection of any plain vanilla chaotic system such as the Lorenz map or Logistic map to produce a pseudo-random sequence to encrypt the watermark before embedding it into the host image. They also enhance the security since a slight alteration of the chaotic parameters will make it difficult for the attacker to identify any sign of the watermark or even to eliminate it. When used in conjunction with conventional watermarking schemes the use of chaotic encryption guarantees the robustness of the watermark message against attacks such as addition of noise, crops or compression while at the same time ensuring that the watermark is invisible within the image. This method turns out to be most useful for the applications where security is of high level such as the protection of copy rights, authentication, and detecting tampering.

III. PROPOSED METHOD

The proposed work contains a method of shares building from the original colour image and a watermark for a safe embedding of the watermark. It starts with the partitioning of the input image, the watermark, both of size 256 × 256 pixels into blocks of size 16 × 16 pixels and produces 256 smaller blocks altogether. In this case, multi-directional features are obtained by employing the WHT and texture features are obtained by employing the LBP while the multiscale features are obtained by employing the DWT for every block. These feature vectors are then stacked to another feature vector, reshaped into a block with the size of original (16 × 16 pixels) and located in the right position of a feature share image constructing a complete feature share (Fs) of the size 256 x 256 pixels.

Second, using the same stream generator, a key share (Ks) of the same size is created mathematically. The secret share (SS) is also calculated by taking the exclusive OR of the two shares modulus 2^8-1 that is the feature share (Fs) and the key share (Ks) where '~' represents the watermark. The secret share is stored with a TA in a secure manner and can be retrieved in the future; the key share is revealed in private to the owner of the images. Last step is the displaying the watermarked image and the watermark so that the method adopted to water mark the image should be secure and cannot be tampered easily.

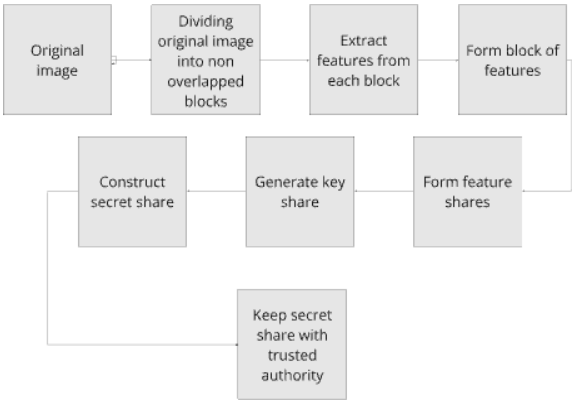

***Fig: 1** Block diagram of the proposed method: Shares construction phase*

The method used to detect forgery in a color image is as follows to check how much similarity is between the received forged image and the original watermark and shares. At this stage, the forged image (FI), secret share (SS), key share (Ks), and the original watermark (W) are partitioned into 16 X 16 blocks; this makes each of them to have 256 blocks.

Multi-directional features are characterized from each block of the forged image using the Walsh–Hadamard Transform (WHT); For texture features, the Local Binary Patterns (LBP) are used; For multiscale features, the Discrete Wavelet Transform (DWT) is used. These feature vectors are combined and reshaped into blocks of equivalent dimension (16×16 pixels) that constitute a feature share which is Fs. The key share, (Ks) is generated from the image owner while the secret share (SS) is obtained from trusted authority.

By employing the elements of the marked signal, the watermark is reconstructed by performing an exclusive OR operation to the secret share, the feature share and the key share. This recovered watermark is then compared, with the original watermark which is also arranged in 16 × 16 macro blocks. The procedure of checking each block's validity involves, comparing the corresponding blocks in the recovered watermark to that of the original watermark. If these two pieces of blocks are the same, then the corresponding entry in the Forged Regions Matrix (FRM) is set to 0 which means that it is authentic. In the case that it does not match, the entry is set to 1 that is forged.

The final blocks after scanning all the blocks are adopted where all the outlier blocks are distinguished in order to enhance the forgery detection. In other words, if all the entries of the FRM matrix are zeros the image is accepted as original with no sign of forgery. If not, the image is considered forged and the matrix provide the information of the forged regions. The advantage of this method is that it delivers a solid constructive approach for forgery detection and localization in images.

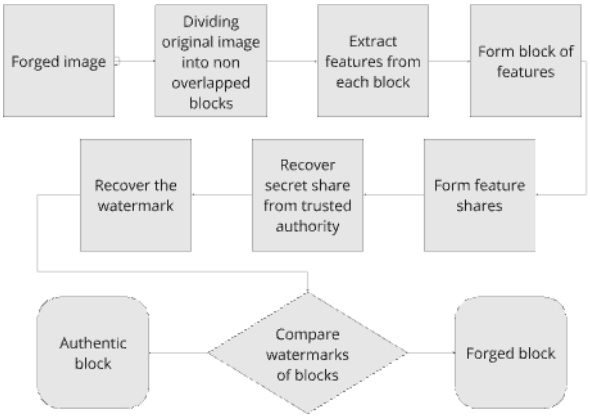

***Fig: 2** Image forgery verification*

IV. IMPLEMENTATION

This implementation describes a watermarking and forgery detection system that uses several Python libraries like Opencv, NumPy, Pywavelets, skimage. The system also enables the insertion of watermarks in images, ability to determine whether an image has been tampered with or not, and ability to determine the quality of an image through use of different image processing techniques.

Libraries and image processing techniques:

OpenCV: OpenCV has an imperative part in image manipulation in which it affords sundry operations including reading, resizing, splitting and joining colour channels- these are core operations in an image processing. Using cv2.imread(): images can be brought into memory from different file formats of images e.g. JPEG or PNG images which are easily manageable objects in the form of NumPy arrays. Once an image is loaded, change a size to other dimensions frequently used in image processing is possible with cv2.resize(), which enables scaling along with preserving or changing aspect ratios are also supported. For colour manipulation OpenCV provides cv2.split() splits an image into separate channels such as red , green and Blue in images that are in RGB format and it is useful for processing of individual channel. Similarly, cv2.merge() – This function recombines the separated channels of an image after some change has been done to it. Both in terms of reading an image and resizing it as well as channel manipulation, OpenCV proves to be quite flexible and versatile to cater to images in different formats and requirements such as object detection, image transformations and real time processing.

NumPY: It is a library that is indispensable to Python in the sphere of numerical computing, which provides a lot of potential in matrix calculations and pixel manipulation of the images. Since image processing is one of the major subsets of real-world signal processing tasks, NumPy uses multi-dimensional arrays to store images, where each value in the matrix correspond to pixel intensity. Such representation enables computationally intensive tasks like mathematical operations, data filtering and transformations, and even aggregation in terms of vectors. For example, with NumPy, one can easily add, multiply, or divide all the corresponding elements in two given arrays as well as apply any mathematical function to each element of an array and perform tasks like image convolutions and Fourier transformations. Due to the backend support of NumPy, working with lists which is natively supported in Python become computationally intensive or time consuming for manipulation of image data and with the help of NumPy such operations become quite efficient. This feature is especially important for real-time applications, where often large images or video frames have to be processed on the fly and for complex image processing scenarios.

You can get other utilities such as Local Binary Patterns (LBP), Structural Similarity Index (SSIM) and the Peak Signal to Noise Ratio (PSNR) from Skimage. PyWavelets fulfills the necessities for applying DWT in order to extract vital features in the frequency domain of image blocks. Fourier submodules of SciPy are used for performing FWHT and DCT.

Watermark Embedding :

The first step involves partitioning of the input image by a function divide image into blocks, which partitions the image into 16×16 blocks and makes it easier to embed watermarks in small portions of the image. Then, for each block, the system extracts features by applying several transforms to it next, the system analyzes the resulting feature set. Cohere features in the frequency domain are captured by the FWHT (implemented in fwht()). Local Binary Pattern (LBP), Local binary pattern is performed through skimage package. feature. local_binary_pattern(), extracts texture information. Last but not the least, Discrete Wavelet Transform (DWT) (using function pywt.dwt2()) takes both frequency and position characteristics into consideration.

The watermark embedding function, the embed_watermark() function makes sure that the watermark and the standard image dimensions are identical. After that, for each image block the extracted features are normalized to form a feature matrix. F. Then we created a random key K, the watermark W
The W is embedded by XORing F,K,S.

Watermark Extraction and Forgery Detection:

There is a detect_forgery() function that allows detecting the forgery starting with extracting the corresponding features from the supposed to be forged image in the manner similar to the features extraction during the embedding. The extracted features are exclusive-OR with the key K and the watermarked image S; disparities between blocks in the extracted watermark and the original are presented as forgery risk map (FRM). The system detects the genuine blocks that contain the watermark and the forging blocks which don't contain or have deviations from the original watermark. If the colour and type of all the blocks matches then the image is considered to be genuine. Otherwise, the FRM tags the forged blocks for more investigation on its part as a fraudulent detection model.

It is an implementation of a number of techniques for embedding, extracting and verifying the watermarks using Python language and a number of image processing tools. These include OpenCV, NumPy, Skimage and PyWavelets that facilitate handling of images and implementing feature extraction or block manipulation efficiently. This makes the design of the system complete by adding two standard image quality metrics namely peak signal to noise ratio (PSNR), structural similarity index (SSIM) as well as bit error rate (BER) giving a proper way for watermarking as well as forgery detection in grayscale as well as colored images.

V. EXPERIMENTAL RESULTS

**** PSNR (Peak Signal-to-Noise Ratio)***:
50.649 dB -This is an excessive fee, suggesting that the modifications between the original and the solid photo are minimum and almost unnoticeable to the human eye.
**** SSIM (Structural Similarity Index):***
0.999 – The SSIM may be very close to 1, indicating that the shape of the picture has been well preserved, notwithstanding the forgery.
**** BER (Bit Error Rate):***
0.128 – This incredibly low price implies fewer bit-level errors among the unique and the watermarked picture as compared to the primary case, wherein BER turned into significantly better.

The result indicates whether the photograph has been solid or no longer. It also offers us with a binary matrix which localizes the forged blocks of a solid photograph. Here the 1's within the matrix indicate the cast blocks. We can calculate the Forgery Rate Metric (FRM) by means of analysing the proportion of the picture that has been solid. The Forgery Rate Metric (FRM) is a crucial measure used to assess the robustness of watermarking schemes towards forgery assaults in digital pics.
To calculate the FRM, a binary matrix representing the image and the solid blocks is analysed. In this matrix, blocks recognized as cast are marked with 1s, even as unaltered blocks are marked with 0s. The overall wide variety of blocks in the picture is determined, and the quantity of solid blocks is counted by means of summing the 1s within the matrix. The FRM is then calculated because the ratio of cast blocks to the total quantity of blocks, imparting a quantifiable metric that shows the quantity of forgery in the photo. For example, if a photo matrix has 16x16 blocks and the forged blocks are without a doubt recognized, the FRM may be computed to understand the share of the picture that has been tampered with. This metric is important for assessing the effectiveness of watermarking strategies in defensive virtual content material towards unauthorized changes.

***Fig: 3** Original Image*

***Fig: 4** Watermark*

Fig: 5 *Watermarked Image*

Fig: 6 *Forged Image*

```
Image is forged and the forged blocks are identified in the FRM
[[1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0]
 [1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0]
 [1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0]
 [1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0]
 [1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1]
 [0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1]
 [0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1]
 [0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1]]
PSNR: 50.649060610378534 dB
SSIM: 0.999360353105161 9
Bit Error Rate (BER): 0.12857627868652344
```

Fig:7 *Final result and FRM*

VI. COMPARISION TO PREVIOUSLY PROPOSED METHODS

A visual cryptography-based watermarking approach that introduces a secure and precise based method for the detection and localizing the image forgery is different by splitting an image into encrypted shares. The watermark is hidden inside the shares of an image in this tactic in order to- be found only if we do the addition of these shares in the right way and here the concept of the watermark is put into practice at its best. Therefore, the watermarking in this method is highly secured in that neither the watermark nor the image is tampered with. Therefore, the image tampering is not possible. Only the image if it is wrong must be combined with the wrong shares that the watermark is reconstructed wrong. If, for example, the watermark is not able to be correctly reconstructed by the shares, when the shares are used, the image will be successfully manipulated. This illustrates why traditional watermarking, like spatial and frequency domain techniques, are commonly implemented for the embedding of watermarks in the pixel or transform coefficients of an image. However, the data embedding methods, such as the waveform-based data hiding, are very sensitive to attacks and therefore are more complex and expensive than simpler methods are. These methods are less prone to such processing and can continue to be used for compression, noise, filtering, and cropping. The "detection only" approach also has the drawback of being more generalized and may need additional algorithms for the identification of the regions of forgery.

However, it should be noted that visual crypto watermarking not only is good in detection of forgery but also localizes these wrong changes quite well. The method is based on the knowledge of secret differences between the sharers who can be used to- find the designation of areas, which were edited and to- be processed. Such a distant stage of localization inconveniences the use of traditional manner. Nevertheless, the other guarantee and accuracy are that they face the additional video that means the shares need more resources to manage it so the- problem- with the high- tech polymerase chain is greatly popularized. The strength of visual cryptography against resizing, compressing, and geometric transformations is even greater than when using other methods, Thus, it is an excellent alternative to applications that are sensitive to image authenticity such as legal evidence, medical imaging, and digital forensics. The previous model was not as successful in safeguarding data authenticity and detecting tampering as this new one due to the capacity of the image to be resized and the watermark to be successfully detected.

VII. CONCLUSION

Thus, the use of hardware for the photo forgery detection and localization with the aid of way often called visual cryptography – primarily based watermarking approach is confirmed to be each reliable and efficient. Since the concept of visible cryptography is applied in imposing the answer, it will become feasible to create watermarks that humans can fast and easily check without severe computation. Watermarking system includes placing one or greater shares of a binary watermark into the host photograph with the least loss within the best of the photo Forensic evaluation is simplified: for the purpose of later checking the validity of the suspect photograph, the stocks that the suspect picture try and embed into it are extracted and the authentic stocks are placed on pinnacle of the extracted stocks. An undistorted watermark on the original role proves the document's genuineness, while its distortion may additionally reveal manipulation. In the same way, this method can help in achieving accurate localization of forgery because of the block- wise insertion of the watermark that in line with block can be assessed for authenticity. This makes it applicable in very steady and high integrity programs of visible information together with law enforcement, medical use, and communications.
Hence, there may be the concept for the usage of visual cryptography based totally watermarking that is found to be provably secure, simple and has the capability to guard visible information from forgery and tampering in numerous essential packages.

ADDRESSING CHALLENGES AND FUTURE RECOMMENDATIONS:

The limitations of visual cryptography-based watermarking include vulnerability to several attacks like compression and others, scaling, cropping, addition of noise and the like. Thus, improving the overall stability can be obtained by placing the watermark in the frequency domain (for example, DCT or DWT), which will be more resistant to the above actions. Staying right in the middle of the visible zone and the antagonistic strength of the watermark is also a very important factor. To satisfy both goals using a single image adaptively, adaptive watermarking techniques can be of great use since they adapt the watermark to the area where it is going to be placed according to local characteristics of the image. Another issue that watermarks face is the level of difficulty and time required for extraction of the watermark which has complications and therefore requires the establishment of efficient algorithms without compromising on the degree of detection. Also, one needs to minimize the cases of false positives, that is, when authentic images are considered as tampered and false negatives, when images that were actually altered are considered non-tampered, which can be solved through using complex error correction and detection codes.

Future recommendations for improving visual cryptography-based watermarking include integrating AI and machine learning techniques to enhance forgery detection and localization. Combining visual cryptography with other watermarking methods, such as robust hashing or spread spectrum watermarking, can leverage the strengths of multiple techniques. Developing real-time watermarking and forgery detection systems is essential for applications requiring immediate verification, such as live video streaming and surveillance. Creating user-friendly tools and interfaces will facilitate broader adoption across various industries. Promoting the standardization of these techniques ensures interoperability between different systems and platforms, enhancing usability and integration. Lastly, developing privacy-preserving watermarking methods, especially for sensitive applications like medical imaging and legal evidence, can protect the content while allowing for effective watermarking. Addressing these challenges and following these recommendations will significantly enhance the reliability and robustness of visual cryptography-based watermarking for a wide range of application.

REFERENCES

[1] Fridrich, A.J.; Soukal, B.D.; Lukáš, A.J. Detection of copy-move forgery in digitalimages. In Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, USA, 6–8 August 2003; pp. 1–10. [Google Scholar]

[2] Hany, F. Image forgery detection. IEEE Signal Process Mag. 2009, 26, 16–25. [Google Scholar]

[3] Asghar, K.; Habib, Z.; Hussain, M. Copy-move and splicing image forgery detection and localization techniques: A review. Aust. J. Forensic Sci. 2017, 49, 281–307. [Google Scholar] [CrossRef]

[4] Yousif, S.F.; Abboud, A.J.; Radhi, H.Y. Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory. IEEE Access 2020, 8, 155184–155209. [Google Scholar] [CrossRef]

[5] Ulutas, G.; Ustubioglu, A.; Ustubioglu, B.; Nabiyev, V.V.; Ulutas, M. Medical image tamper detection based on passive image authentication. J. Digit. Imaging 2017, 30, 695–709. [Google Scholar] [CrossRef] [PubMed]

[6] Li, J.; Li, X.; Yang, B.; Sun, X. Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. 2014, 10, 507–518. [Google Scholar]

[7] Gul, E.; Ozturk, S. A novel hash function based fragile watermarking method for image integrity. Multimed. Tools. Appl. 2019, 78, 17701–17718. [Google Scholar] [CrossRef]