Image Authentication based on Histogram Shifting Method using Arnold's Cat Map

RAMAKRISHNA MISSION RESIDENTIAL COLLEGE(AUTONOMOUS),
NARENDRAPUR, KOLKATA - 700103

B.Sc. Sixth Semester Examination, 2024

Subject: Computer Science

Paper: DSE04 (Project)

Submitted by:

Niladri Ghosh
Registration No: A03-1112-0179-21
Roll No: 6R24CMSA2002

Arnab Bera
Registration No: A03-1142-0187-21
Roll No: 6R24CMSA2008

Supervised by:

Sri Bibek Ranjan Ghosh

Submitted on: May 21, 2024

Acknowledgment

It is our great pleasure to express our profound sense of gratitude to our esteemed Supervisor Sri Bibek Ranjan Ghosh, for providing his constructive academic advice and guidance, constant encouragement, and valuable suggestions at crucial junctures and all other support throughout this project work, and for helping us to prepare the project report successfully. We really benefited from his excellent supervision. We would extend our sincere thanks to our respected Head of the Department. Dr. Siddhartha Banerjee, for allowing us to use the facilities available. I would like to thank our lab assistant Shyamaprosad Chakravorty & teachers of our department for extending this wonderful opportunity of working on a project as our DSE-4 in our curriculum.

Certificate

I hereby certify that the project report titled Image Authentication based on Histogram Shifting Method using Arnold's Cat Map." which is submitted by Niladri Ghosh (Registration No: A03-1112-0179-21, Roll No: 6R24CMSA2002), Arnab Bera (Registration No: A03-1142-0187-21, Roll No: 6R24CMSA2008) to the faculty of the Computer Science Department of Ramakrishna Mission Residential College in Complete fulfilment of the requirements for the Degree of Bachelor of Science (Honours) in Computer Science, is a record of the project work carried out by the students under my supervision in the academic session of the final semester (semester VI) of 2023- 2024.

(Signature of Head of the Department) (Signature of Supervisor)

INDEX

Problem Description

Digital watermarking is a crucial technique for embedding and extracting hidden information in digital media, including medical images. Image authentication plays a critical role in ensuring the integrity and authenticity of digital medical images, which are essential for accurate diagnosis, treatment planning, and research. The project focuses on the development of a robust watermarking algorithm for images authentication using methods, including techniques like Haar Transform, Histogram Shifting, Arnold's Cat Map. The methods aim to embed an imperceptible watermark into images, which can later be extracted to verify the authenticity and integrity of the images.

Chapter 1: Introduction

1.1 Steganography:

Steganography is the technique of hiding secret data within ordinary, non-secret files or messages to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data

After the data is protected in the cover image, the secret data is extracted from the stego image. Perfectly reconstructing the secret data along with the cover image is called reversible steganography.

The word steganography is derived from the Greek word ‘steganos ‘(hidden or covered) and ‘graph’(write)

In digital steganographic systems, the fundamental requirement is that the stego-image be perceptually indistinguishable to the degree that it does not raise suspicion . In other words, the hidden informationally briefly modifies to the cover object. Most passive wardens detect the stego-images by analysing their statistical features.

In general, steganalytic systems can be categorized into two classes: spatial domain steganalytic systems (SDSSs) and frequency domain steganalytic systems (FDSSs).

SDSSs are adopted for checking lossless compressed images by analysing the statistical features of the spatial domain. For lossy compressed images, such as JPEG files, FDSSs are used to analyse the statistical features of the frequency domain.

1.2 Watermarking:

Watermarking is a technique with similarities to steganography. It has been around for centuries and is commonly used in money and stamps to assist in identifying counterfeiting. The idea behind watermarking is to create a translucent image on the paper to provide authenticity. Since mailing letters was far more expensive centuries back, it was common for

people to use counterfeit stamps on their mail. For example, a translucent elephant watermark was used on stamps in India to deter counterfeiting.

Digital watermarking is used to maintain ownership and authenticity of digital media such as music and videos.

It is important to note that although watermarking has many similarities to steganography in terms of embedding data, but the intent of watermarking is not to make it difficult to detect that embedded data, but rather make it difficult to remove the embedded data so as to prevent the unauthorized reuse of the file.

Watermarking is of two types; visible watermarking and invisible watermarking.

Visible Watermarking, that refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text. For example, in a TV broadcast, the logo of the broadcaster is visible at the right side of the screen. And Invisible Watermarking, that refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

1.3 Basic model of Steganography

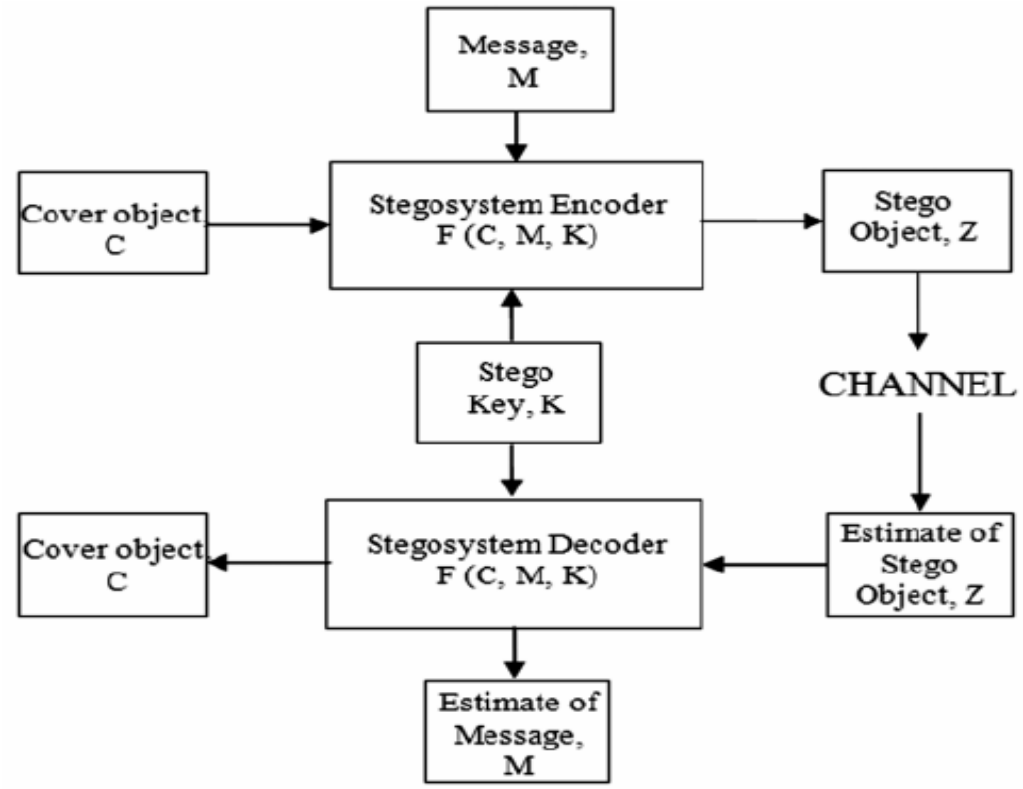

Figure 1: Basic model of steganography

1.4 Characteristics of Steganography:

In steganography, the message to be hidden inside the cover–media must consider the following features.

1.4.1 Hiding Capacity: This feature deals with the size of information that can be hidden inside the cover file. A larger hiding capacity allows the use of a small cover and thus reduces the bandwidth required to transmit the stego–media. For example, if we have an RGB image with a size of 200 x 200 pixels, that means that we have 120,000 colour values to be used as cover values for the secret message (200:width x 200:height x 3:R,G,B), then if we use only one bit per colour channel for hiding the message we have a hiding capacity of 120,000 bits or 15,000 bytes, if we use 2 bits per colour channel for hiding the message we have 30,000 bytes, but if we use only one colour channel and one bit per pixel, the hiding capacity will be 40000 bits or 5000 bytes.

1.4.2 Perceptual Transparency: Perceptual transparency is an important feature of steganography. Each cover-media has certain information hiding capacity. If more information or data is hidden inside the cover, then it results in degradation of the cover–media. As a result, the stego–media and cover–media will appear to be different. If the attacker notices this distortion, then our steganographic technique fails and there is the possibility that our original message can be extracted or damaged by the attacker

1.4.3 Robustness: Robustness is the ability of the hidden message to remain undamaged even if the stego–media undergoes transformation, sharpening, linear and non-linear filtering, scaling and blurring, cropping and various other techniques

1.4.4 Tamper–resistance: Of all the features, this feature is very important. This is because, if the attacker is successful in destroying the steganographic technique then the tamper–resistance property makes it difficult for the attacker or pirates to alter or damage the original data.

1.5 Image Steganographic Techniques:

steganography techniques can be divided into following domains

1.5.1 Spatial Domain Methods: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)

2. Pixel value differencing (PVD)

3. Edges based data embedding method (EBE)

4. Random pixel embedding method (RPE)

5. Mapping pixel to hidden data method

6. Labelling or connectivity method

7. Pixel intensity-based method

8. Texture based method

9. Histogram shifting methods

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.

2. More information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.

2. Hidden data can be easily destroyed by simple attacks.

1.5.2 Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).

2. Discrete cosine transformation technique (DCT).

3. Discrete Wavelet transformation technique (DWT).

4. Lossless or reversible method (DCT)

5. Embedding in coefficient bits

1.6 Performance metrics for image watermarking:

Various methods are used to evaluate the quality of image watermarking. Each of these methods assesses a different aspect of the result obtained after watermarking. Some of the well-known methods are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structured Similarity Index Measure (SSIM), Payload Capacity[12][13].

1.6.1 Payload capacity:

Payload capacity refers to the measure of the volume of information present within the cover image. This measure is important in a steganographic system as the communication overhead depends on the maximum payload capacity. It is measured in Bits Per Pixel (BPP).
BPP = NUMBER OF SECRET BITS EMBEDDED/ TOTAL NUMBER OF PIXELS

1.6.2 Mean Square Error (MSE):

Mean Square Error is the averaged value of the square of the pixel-by-pixel difference between the original image and stego-image. It gives us a measure of the error produced in the cover image due to the data embedding process.

$$\mathrm{MSE}\ (q1, q2) = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (q_1(i,j) - q_2(i,j))^2$$

Equation 1: Mean Square Error

M, N = Dimensions of the image

I = Original Image

K = stego-image

Where q_1 (i, j) and q_2 (i, j) indicate the original and extracted images, respectively.

Note:
Lower value of MSE indicates good quality of embedding.

1.6.3 Peak Signal to Noise Ratio (PSNR):

PSNR is another popular way to measure the degree of distortion in the cover image due to embedding. It is the ratio between the maximum possible value of a signal and the power of distortion noise (MSE). It is measured in dbs.

PSNR = 10xlog (Max^2/MSE)

Max = 255 for an 8-bit grayscale image

Note:

A higher value of PSNR indicates a better-quality embedding.

1.6.4 Structured Similarity Index Measurement (SSIM):

SSIM is a metric of comparison to check the similarity between the cover image and stego-image. It measures the perceptual difference between the two images.

$SSIM= (2\mu_x\mu_y + c_1)(2\sigma_{xy} +c_2)/((\mu_x)^2+(\mu_y)^2 +c_1)((\sigma_x)^2 +(\sigma_y)^2 + c_2)$

c_1 and c_2 are the two stabilizing parameters,

$c_1 = (k_1L)^2$

$c_2 = (k_2L)^2$

L is the dynamic range of pixel values $(2^{\#bits\ per\ pixel} - 1)$

Let the contents, k_1=0.01 and k_2=0.03.

μ_x and μ_y are the mean intensity values of images x and y.

$(\sigma_x)^2$ is the variance of x,

$(\sigma_y)^2$ is the variance of y

$(\sigma_{xy})^2$ is the covariance of x and y.

Note:

SSIM value close to 1 indicates good quality.

1.6.5 Normalized Cross Correlation (NCC):

It involves computing the similarity between two images by sliding a window over the images and comparing the pixel values within the window.

The similarity is computed using the cross-correlation formula, which involves multiplying the corresponding pixel values in the two images and summing the results. The result is then normalized to obtain a value between -1 and 1, which indicates the degree of similarity between the two images.

$$NCC = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}(I_c(i,j)\ I_s(i,j))}{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}(I_c^2\ (i,j))}$$

Equation 2: Equation of NCC

Here, M is row , N is column, I_c is cover image and I_s is stego image.

Target of performance as a whole:
A low MSE (close to 0), high PSNR(>30dB) and high SSIM value (nearly 1) is desired as a result.

1.7 Discrete Wavelet transformation technique (DWT):

DWT stands for Discrete Wavelet Transform, which is a mathematical transformation that analyzes signals and data in terms of their frequency components and time localization. It breaks down a signal into its constituent wavelets, which are small wave-like functions that are scaled and translated to capture different frequencies and time intervals of the original signal.
The DWT is widely used in signal processing, data compression, image and audio processing, and other fields where the efficient representation of signals in a compact form is essential. It has numerous applications in areas such as image and video compression, denoising, feature extraction, and pattern recognition.

The DWT has several advantages over other signal processing techniques, such as the Fourier transform, because it can capture both time and frequency information simultaneously, and it can handle non-stationary signals with varying frequency content [11].

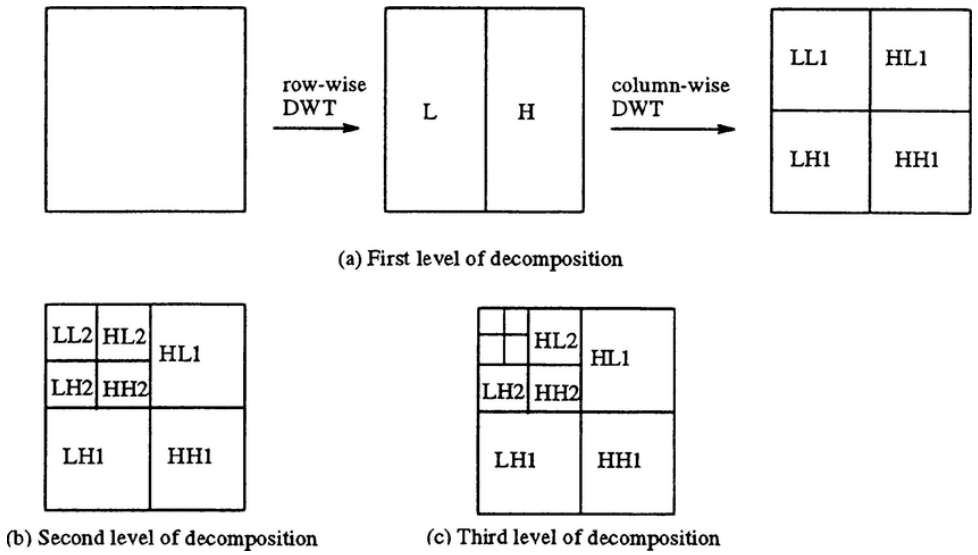

Figure 2: 2D DWT Example

1.8 Haar Transform:

The Haar transformation is a mathematical technique used in signal processing and image analysis, forming the basis of the Haar wavelet transform. It was introduced by Alfred Haar in 1909 and is one of the simplest and most fundamental forms of wavelet transform. The Haar transform is particularly valuable due to its simplicity, computational efficiency, and ability to handle both continuous and discrete data.

The Haar transformation operates by decomposing a signal into its average and difference components, using a pair of orthogonal basis functions: the Haar wavelet and its scaling function. The Haar wavelet is characterized by a step function that takes on values of 1 and -1, while the scaling function is a simple rectangular pulse. Mathematically, for a given signal $f(t)$, the Haar transform can be represented as a series of scaling coefficients and wavelet coefficients, which describe the signal's low-frequency (average) and high-frequency (difference) components, respectively.

The Haar transform is widely used in various applications due to its efficiency and simplicity. In image processing, it is used for tasks such as image compression, denoising, and edge detection. For example, the JPEG 2000 image compression standard employs wavelet transforms, including the Haar transform, to efficiently compress images by representing

them with fewer coefficients while preserving important features. In signal processing, the Haar transform helps analyses time-series data, detecting changes and trends by examining the differences at various scales.

The Haar wavelet's mother wavelet function $\psi(t)$ can be described as-

$$\psi(t) = \begin{cases} 1 & 0 \leq t < \frac{1}{2}, \\ -1 & \frac{1}{2} \leq t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Its scaling function $\varphi(t)$ can be described as-

$$\varphi(t) = \begin{cases} 1 & 0 \leq t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

One of the primary advantages of the Haar transform is its computational simplicity. It can be implemented efficiently using a fast algorithm that requires only $O(N)$ operations, making it suitable for real-time applications. Additionally, the Haar transform's ability to handle both continuous and discrete data makes it versatile. However, it also has limitations; its blocky step function basis can lead to artifacts in the transformed signal, particularly in image processing where smooth transitions are common. Despite these drawbacks, the Haar transform remains a fundamental tool in signal and image analysis, often serving as a stepping stone to more complex wavelet transforms.

1.9 Histogram Shifting:

Histogram shifting is a reversible data hiding technique used in image processing that involves modifying the histogram of pixel intensities to embed information without significantly altering the image quality. This process identifies the peak point (highest frequency intensity) and zero point (intensity with zero or minimal frequency) in the histogram. It then shifts the pixel values between these points to create space for embedding data. Data bits are embedded by slightly modifying the pixel values at the peak point, ensuring the hidden data can be extracted later. After data extraction, the original image can be perfectly restored by reversing the histogram shift, preserving the original image quality.

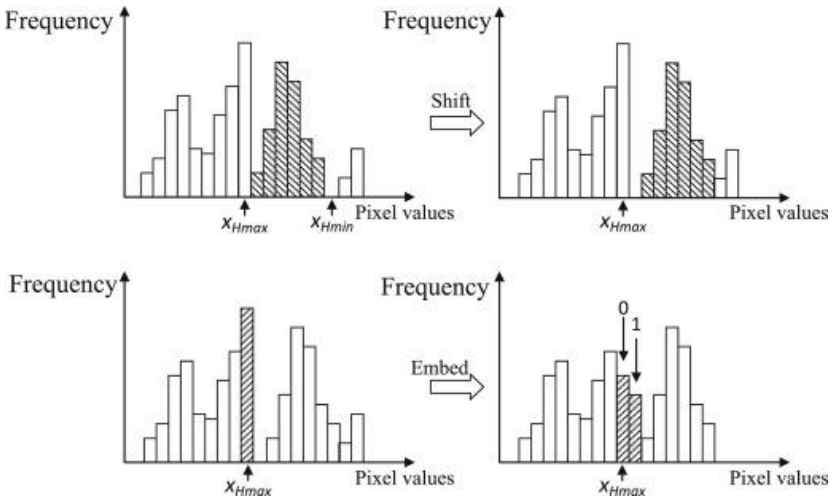

Figure 3: Singular value Decomposition

1.10 Arnold's Cat Map:

In mathematics, Arnold's cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, hence the name. It is a simple and pedagogical example for hyperbolic toral automorphisms.

Thinking of the torus as the Quotient space, Arnold's Cat Map is given by the formula-

$$\Gamma(x, y) = (2x + y, x + y) \backslash mod 1$$

Equivalently the matrix notation is-

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1.$$

That is, with a unit equal to the width of the square image, the image is sheared one unit up, then two units to the right, and all that lies outside that unit square is shifted back by the unit until it is within the square.

1.10 SHA 256:

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that outputs a fixed-size 256-bit hash from an input message, irrespective of its length. As part of the SHA-2 family, developed by the National Security Agency (NSA) and standardized by the National

Institute of Standards and Technology (NIST), SHA-256 is extensively utilized in security protocols and applications, such as SSL/TLS, digital signatures, and blockchain technologies. The algorithm ensures data integrity and authenticity through its key properties: producing a consistent hash value for the same input, making it infeasible to reverse-engineer the original message from the hash (preimage resistance), and ensuring that even a tiny change in the input results in a significantly different hash (avalanche effect).

The SHA-256 process involves several steps, beginning with padding the input message to ensure its length is a multiple of 512 bits, followed by dividing the message into 512-bit blocks. Each block undergoes a series of 64 rounds of complex operations involving bitwise logical functions and modular additions, using a set of initial hash values and constant values derived from the first eight prime numbers. These operations iteratively update the hash values, culminating in the final 256-bit hash output after all blocks are processed. SHA-256's robust design and computational efficiency make it a cornerstone of modern cryptographic practices, providing essential security features for data integrity and digital verification.

1.11 Security Analysis:

1.11.1 Passive attack:

Image steganalysis is a binary pattern classification process whose objective is to correctly distinguish a stego image from a clean one. Broadly, it can be based on the knowledge of the steganographic algorithm behind or without it. The former is specific steganalysis and the latter is universal or blind steganalysis.[18] It is the process of detecting steganography. Basically, there are two methods of detecting modified files. One is called visual analysis, which involves comparing a suspected file with the original copy. It intends to reveal the presence of secret communication through inspection, either by eyes or with the help of a computer system, typically decomposing the image into its bit planes. Although this method is very simple, it is not very effective; most of the time, the original copy is unavailable. [5]

1.11.2 Active attack:

1.11.2.1 Gaussian Filter Attack:

The idea of blurring is to decrease the magnitude of high-frequency components. A low-pass filter in the frequency domain is equivalent to a mountain shape in the spatial domain.

Therefore, a smoothing filter in the spatial domain should have all positive coefficients, with the largest in the centre. The simplest low-pass filter would be a mask with all coefficients having a value of 1. [5] A sample 3 × 3 Gaussian filter is: $\frac{1}{12}\begin{bmatrix}1 & 1 & 1\\ 1 & 4 & 1\\ 1 & 1 & 1\end{bmatrix}$

1.11.2.2 Median Filter Attack:

In image enhancement, a median filter is often used to achieve noise reduction rather than blurring. The method is rather simple: we calculate the median of the gray values surrounding the pixel's neighbourhood and assign it to the pixel.[5] The resistance of a watermarked algorithm against mean and median filter depends largely on where the watermark information is embedded. High frequency edge embedding will likely suffer from mean and median filters while low frequency intensity embedding will remain relatively resistant to such filter attacks.

1.11.2.3 JPEG Attack:

JPEG 2000, which is a standard image compression technique created by the JPEG committee, uses the state-of-the-art wavelet-based technology. This creation aims at overcoming the blocky appearance problem occurred in the discrete cosine transform–based JPEG standard. Its architecture has various applications ranging from prepublishing, digital cameras, medical imaging, and other industrial imaging. In general, JPEG 2000 is able to achieve a high compression ratio and simultaneously avoid blocky and blurry artifacts. [5]

1.11.2.4 Salt & Pepper Attack:

Salt and pepper noise refers to a wide variety of processes that result in the same basic image degradation: only a few pixels are noisy, but they are very noisy. The effect is similar to sprinkling white and black dots—salt and pepper—on the image. By randomizing which pixels are changed, the noise is scattered throughout the image. The combination of these randomizations creates the "salt and pepper" effect throughout the image.

1.11.2.5 Crop Attack:

A crop attack on watermarking refers to a specific type of digital image manipulation aimed at removing or altering watermarks applied to images for copyright or ownership protection.

Watermarking is a technique used to embed a visible or invisible marker into digital media, such as images, to identify the copyright holder or the owner of the content. The goal of a crop attack on watermarking is usually to evade detection or claim ownership of the image without proper authorization. It is commonly employed by individuals or entities seeking to use copyrighted images without permission or to misrepresent ownership.

1.11.2.6 Histogram Equalization Attack:

Histogram Equalization is a computer image processing technique used to improve contrast in images. It accomplishes this by effectively spreading out the most frequent intensity values, i.e., stretching out the intensity range of the image. This method usually increases the global contrast of images when its usable data is represented by close contrast values. This allows for areas of lower local contrast to gain a higher contrast.

$$s_k = T(r_k) = (L-1)\sum_{j=0}^{k} p_r(r_j) \quad k = 0,1,2,\dots\dots\dots, L-1$$

Equation 3: Histogram Equalization

L is the number of possible intensity levels in an image. Thus a output image is obtained by using the above Eq. to map each pixel in the input image with intensity r_k into a corresponding pixel with level s_k in the output image, is called histogram equalization.

Chapter 2: Literature Survey

1. In this paper a reversible data hiding technique is used by which they perform the difference histogram in between the sub-sampled images by Fragile Mark. This paper has analysed different reversible data hiding algorithms and also analysed the capacity, complexity & visual quality of those algorithms. Then they have showed their proposed algorithm which includes the data embedding process in image & extraction process from the image. They discussed three types of reversible data hiding strategies based on data embedding. First one is to use a lossless compression algorithm to an image to get enough space & there secret message is to be embedded. Second one is to use the transform domain algorithms & the message bit are embedded into their respective coefficients. Third one has two part containing Difference Expansion & Histogram Modification. In Difference Expansion message bits are embedded by enhancing the differences of pixel pairs which we get by the Integer Haar Wavelet Transform and Histogram Modification uses a histogram to embed the message. They try to use the horizontal, vertical & diagonal neighbours of pixel as they have a correlation with more pixel redundancy. In their algorithm they take an image & by performing sub-sampling get a reference sub-sampled image. Prepare empty bins in every histogram of difference images & after shifting the difference histogram, the message is embedded into that and get marked image. Lastly to send overhead information they use LSB with secret key. If marked image is tampered by checking the more occurrence of bins of modify difference histogram with value -1 then stop extraction. Otherwise get the overhead information & determine the reference sub-sampled image. Extract the secret message by creating difference images & then remove the message

from difference image. At last, we get the actual image from marked image through the inverse of the sub-sampling with the sub-sampled image. The marked image will be authentic if the inserted & extracted hash values are totally same. They also provide a solution for the overflow & underflow problem by using modular-256 addition or by using the location map which takes the location of the pixel where problem occurred. To minimise the distortion of pixel flipping they used modular addition with a cycle of length of 64. They measure the distortion by PSNR value in between marked & original image. In their experiment they get largest embedding capacity at sampling factor (3,3) & keeping the distortion at a lowest level. Get better result for Lena, Baboon, Boat, Airplane images with Payload(bits) & PSNR(db)- (20121, 48.9), (6499, 4807), (21442, 48.9) and (32631, 49) respectively. In the all cases they use the values of- Δu, Δv (sub-sampling intervals in a row & column respectively), L (embedding level) to 3, 3, 0 respectively. This algorithm, can avoid salt & pepper noise, is applicable for medical & military images, with embedding capacity ranges in between 6k to 210k. A problem with this algorithm is that its hard to get bpp more than 1 by performing only first round of embedding.

2. In this paper they use Hybrid Domain for Reversible Data Hiding (RDH). A 2D Discrete Wavelet Transform is used to convert the cover image into a transform domain to get the exact frequencies of embedding the payload. The secret message is carried out to the selected DWT coefficients bit planes. They measure the PSNR & SSIM in their experiment. This method also avoids the overflow/underflow problem of the pixel values & get the highest embedding capacity. They use wavelet transform that convert an image from spatial to transform domain but a truncation blunder appeared. It was

solved by integer-to-integer wavelet transform. Discrete wavelet transform (DWT) decomposes an image to four sub bands called LL, LH, HL, HH which are the approximate coefficient of the image. Also, in their proposed method Histogram modification is used to embed the auxiliary data which is used for reversibility of the original image. They use RDH using integer wavelet transform and uses histogram modification with a high payload to provide a low distortion. Basically, they use a hybrid domain for their work. That means secret data is embedded in transform domain using haar transform and auxiliary data is embedded in spatial domain by histogram modification. Getting the pick point from histogram of the image & auxiliary data embedded. Then they preprocess the cover image by haar integer to integer transform. Scan the high & middle frequencies in zig zag pattern to embed the secret data. We they get the replaced frequencies that are stored as auxiliary data (AD). Apply inverse haar transform to get intermediate IHI. While extraction applied histogram to recover auxiliary data. Converting image by haar transform to get secret data from middle & high frequency component and get cover image without any loss by applying inverse integer transform. This method performs well because the scanning was in zig zag pattern & pixel pair coordination is used. For high quality image the Peak Point should be chosen for less bin shifts. The author used the mean result of sixteen medical images of three different type. For hepatitis, pelvic cavity, brain marked images the Bpp, PSNR, SSIM values were better in their proposed method. Though they first tested on baboon image where also they get better result.

3. Abdel-Nabi, Ali Al-Haj, 2017: The paper introduces a joint reversible data hiding and encryption algorithm to secure medical images in telemedicine, ensuring high embedding capacity and low computational complexity. The algorithm divides the image into two halves, embedding a different

watermark in each half—one before encryption and the other after. This method employs substitution-based and transposition-based encryption techniques to achieve high entropy and ensures the original image can be fully recovered. Performance evaluations on 512×512 CT images show the algorithm achieves PSNR values of 56.60 dB for directly decrypted watermarked images, 58.81 dB for partially watermarked images, and infinite PSNR for fully restored images. This indicates the algorithm maintains high image quality while providing robust security and exact recovery capabilities

4. Vinoth Kumar, V. Natarajan 2013: This paper introduces a modified histogram shifting algorithm for reversible medical image watermarking, aimed at increasing data hiding capacity and maintaining high stego-image quality. The approach involves hierarchically dividing the cover image into smaller blocks for data embedding, using a recursive looking-ahead estimation technique to optimize the data hiding volume. This ensures the optimal block division is selected based on hiding capacity, particularly effective for medical images with extensive dark areas. Experimental results demonstrate the efficacy of this method, showing improved PSNR values up to 59.05 for non-recursive and 58.8 for recursive methods. The mean square error (MSE) values range from 0.08 to 0.37, confirming minimal image distortion. This advanced technique enhances the security and integrity of medical images during online sharing, ensuring complete restoration of the original image after data extraction.

5. De Rosal Ignatius, Fadhil 2019: This study introduces an RDH technique using histogram shifting to secure medical images without compromising

diagnostic accuracy. RC4 encryption enhances data security, yielding high PSNR and SSIM scores while increasing entropy. Perfect retrieval of images and data is achieved, ensuring confidentiality during transmission and storage. RDH plays a crucial role in maintaining data integrity and confidentiality in medical imagery. Integration with RC4 encryption advances secure data hiding, protecting patient data effectively. Further research could focus on adaptive methods to minimize histogram shifts based on message capacity. In the paper, the range of values for BPP, MSE, PSNR (dB), and SSIM is as follows:- BPP: 0.0021 to 0.5217, MSE: 0 to 0.9525, PSNR: approximately 48.34 dB to 51.81 dB, SSIM: approximately 0.9855 to 0.9994.

6. Li-Chin Huangc, Lin-Yu Tseng 2013: The paper introduces a reversible data hiding method using histogram shifting for high-quality 16-bit depth medical images. The process involves dividing the image into local pixel blocks, calculating difference values between neighboring pixels to generate a difference histogram, and embedding secret bits by shifting this histogram. This method ensures the original image can be accurately recovered post-extraction. Underflow and overflow issues are managed effectively due to the high bit depth, with specific strategies for signed and unsigned images. The embedding process balances data hiding capacity and image quality by adjusting block size and embedding parameters. Results show PSNR values above 61 dB for signed and 74 dB for unsigned images, maintaining high image quality and structural integrity.

7. Chin-Chen Chang, Thai-Son 2014: The reversible image hiding method outlined in the paper "Reversible Image Hiding for High Image Quality based

on Histogram Shifting and Local Complexity" involves several key stages: preprocessing, histogram shifting, local complexity calculation, peak identification, data embedding, and data extraction/image recovery. Preprocessing includes converting color images to grayscale. The histogram shifting process incorporates identifying smooth and complex image blocks based on a complexity measure and then computing the histogram of difference values to locate peak points. Data embedding involves shifting histogram bins to accommodate secret data, primarily focusing on smooth blocks with higher peak histogram bins. For data extraction and image recovery, the original image and embedded data are restored through inverse histogram shifting. The results section details performance metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). While specific MSE values are not provided, higher PSNR values, such as those reported for the proposed scheme and grayscale Kodak images, imply lower distortion and superior image quality. The paper concludes that the method effectively embeds data with minimal visual distortion, making it suitable for applications requiring high-quality image preservation, such as medical imaging.

8. A. A. Karawia 2021: The paper "Medical image steganographic algorithm via modified LSB method and chaotic map" introduces a method for securely embedding secret medical images into host images for transmission. The algorithm proceeds as follows: the secret medical image undergoes encryption using a one-dimensional chaotic map, followed by the random selection of pixel positions within the host image using a two-dimensional chaotic map. The encrypted bits are then shuffled before being embedded using a modified LSB method, resulting in the creation of the stego image.

Evaluation of host and stego image quality involves metrics such as PSNR, MSE, SSIM, histogram test, image quality measure, and resistance to chi-square attacks. Results demonstrate low MSE, high PSNR values, and high structural similarity (SSIM) between host and stego images, indicating minimal distortion and imperceptibility of embedded data. Overall, the algorithm achieves high visual quality and robustness against attacks, ensuring secure transmission of medical images.

Chapter 3: Proposed Method

Watermarking in medical images is a pretty difficult and very sensitive work. The information of patient should be kept accurately without any error. So, it should be robust against various attacks. For watermark embedding in images different methods are proposed. All have been experimented with SIPI image dataset.

3.1. Image Authentication Based on Histogram Shifting

The first method consists of Haar Transform and based on histogram shifting. Haar Transform is taken for better imperceptibility. At fist an image is divided into many blocks then we process our secret image & text data along with their SHA-256 values to the blocks for the embedding.

3.1.1 Embedding Process

First we take an image then an image then apply forward Haar Transform in the image. We get four components called LL, HL, LH, HH. Then we take our secret image as input & hide it to the HH Component and also hide to SHA-256 value of the secret image in the LL component. For the forward transform we use the equation-

$$a[n]=floor(x[2n]+x[2n+1]/2)$$
$$d[n]=x[2n]-x[2n+1]$$

where, ‘a’ is approx, ‘d’ is detail & x[n] is image pixel locations. We perform this row wise

Before embedding the secret image we change the secret image by Arnold’s Cat Map method to a particular image by setting a certain number of iteration. Then we hide that image.

After hiding the image in block we use the Inverse Haar Transform to get our stego image, We combine the four components which results a stego image. For this we use the equation-

$$X[2n]=a[n]+0.5*(0.5*d[n]+2)$$
$$X[2n+1]=x[2n]-d[n]$$

we perform this in column wise of the image matrix

For a 515x512 size cover image we have taken the secret image of size 16x16. This has been hidden in the cover image. Applying the operation, we get our resultant stego image which we will send to the other hand.

Algorithm1: Embedding (COVER, WI)

Step1: Divide the image into 4parts by forward IWT on COVER image and return components LL, HL, HH

Step2: Apply Arnold's cat map with a specified iteration on WI

Step3: Code WI to SHA-256

Step4: Apply Histogram Shifting technique to hide the secret image in the HH block and SHA-256 code to the LL block

Step5: if find a base point then go to step 6 otherwise stop execution

Step6: Apply the Inverse IWT to the image that results STEGO image

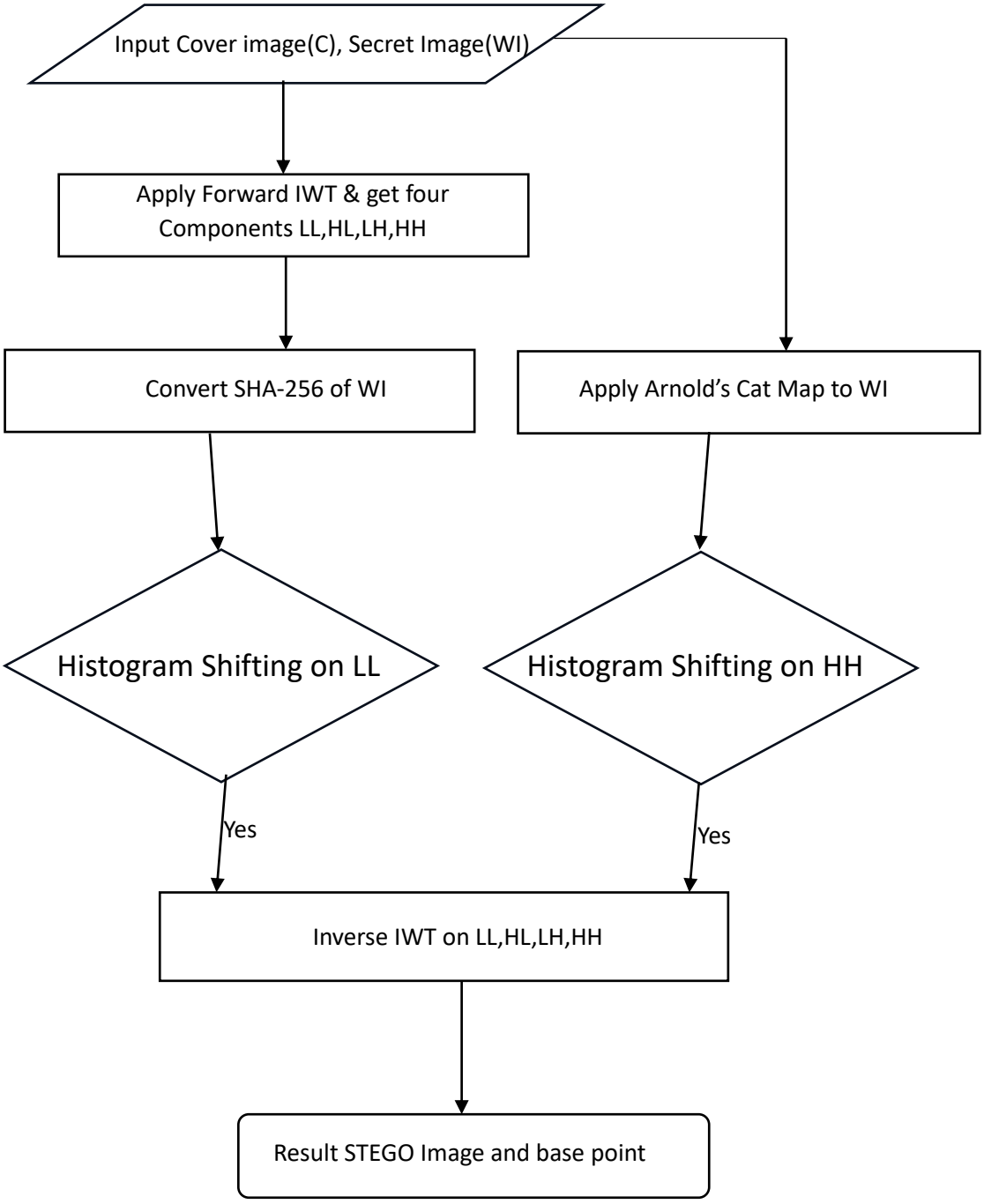

Fig4. Flowchart of Embedding Process

3.1.2 Extraction Process

Doing the same process reversely. 1st applying the forward IWT & get the four components LL, HL, LH, HH. By using the base points we will recover the Secret image from HH component and recover the SHA-256 value from LL component. That's how we will get our secret image from the Stego image.

Algorithm2: Extraction (STEGO, basepoints)

Step1: First, divide the given watermarked image into 4 sub-bands LL, HL, LH & HH using forward IWT

Step2: Take the HH part and apply histogram extraction technique with the basepoint

Step3: extract the secret image

Step4: Apply the Arnold's Cat Map on secret image with remaining iterations to get actual secret image

Step5: Take the LL part and apply histogram extraction technique with the basepoint

Step6: Extract the SHA-256 value

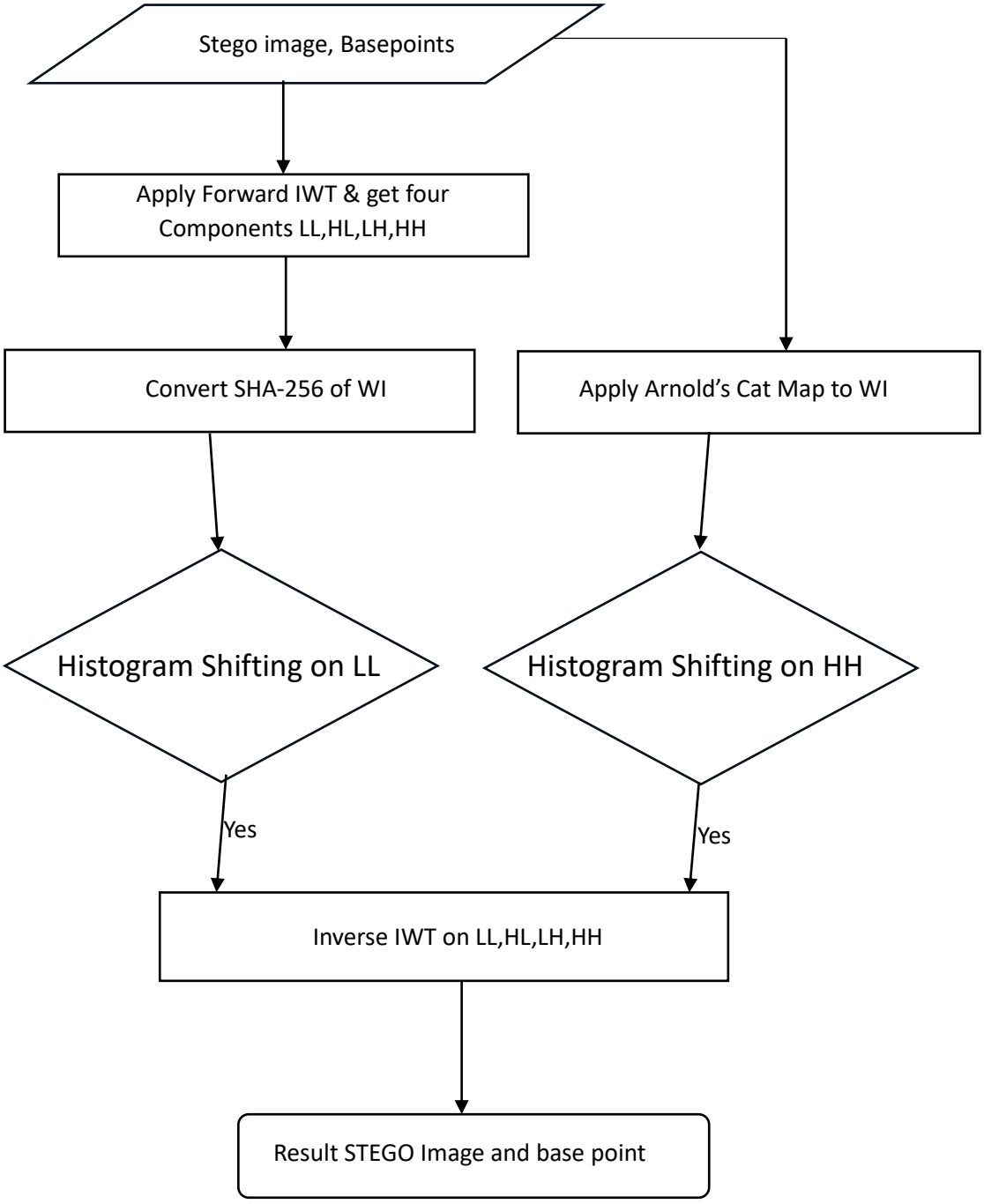

Fig4. Flowchart of Extraction Process

Chapter 4: Experimental Results and Analysis

4.1 Dataset:

The 'USC SIPI Image Dataset' is taken into consideration in this work. In the RESVDUMAUTH method we only use medical image. All images in the USC SIPI database are currently stored in TIFF format. From the official website all the images are taken

4.1.1 USC SIPI Image dataset:

Lena Image Airplane Image Barbara Image

Fig: 10 USC SIPI Image dataset

4.2 Experimental results of Image hiding based Histogram Shifting

This method is experimented using BOSSbase dataset and SIPI dataset, cover image of 512x512 pixels, secret image of size 16x16 pixels. Without any kind of active attack on image, watermark is successfully recovered without any error. Average PSNR of 60.866 dB is achieved. An average NCC of 0.89 is achieved after applying salt & pepper noise of 0.001 density.

Result without Attacks:

Results after embedding without attack on samples images from USC SIPI database-

Cover Image	Secret Image	PSNR	MSE	NCC	SHA
airplane.tiff	splash.tiff	59.53416	0.072388	1	TRUE
Barbara.tif	splash.tiff	61.20761	0.04924	1	TRUE
elaine.tiff	splash.tiff	61.14979	0.0499	1	TRUE
fishingboat.tiff	splash.tiff	60.74799	0.054737	1	TRUE
Goldhill.tif	splash.tiff	61.51282	0.045898	1	TRUE
house.tiff	splash.tiff	60.31865	0.060425	1	TRUE
lena.tiff	splash.tiff	60.40253	0.059269	1	TRUE
peeper.tiff	splash.tiff	61.3544	0.047604	1	TRUE
sailboat.tiff	splash.tiff	61.06172	0.050922	1	TRUE
tank.tiff	splash.tiff	61.37709	0.047356	1	TRUE

Result on Attack:

Results after embedding with attack of on samples images from USC SIPI database. We performed attacks Histogram Equalization, Median Filtering, kernel size=3x3, Gaussian filter with sigma (standard deviation) = 1, Salt & Pepper noise with density=0.001, Gaussian Noise with variance=0.005, Apply Image Sharpening, Average Filtering, Image Resizing with scale=0.5, JPEG Compression with 90%.

Applying this attack on lena.tiff image we get result of PSNR(db)-

'Histogram Equalization PSNR': 19.449399463903944, 'Median Filter PSNR': 35.57826816 212173, 'Gaussian Filter PSNR': 33.2094206805797

And the NCC values are-

Histogram Equalization NCC: : 0.7996339201927185 Median Filter NCC: : 0.8162925243377686 Gaussian Filter NCC: : 0.8043195009231567 Salt & Pepper NCC: : 0.8751115798950195 Gaussian Noise NCC: : 0.843795120716095 Sharpnening NCC: : 0.7500759363174438 Average Image NCC: : 0.7895184755325317 Resize Image NCC: : 0.8481584787368774 JPEG Image NCC: : 0.8365207314491272

Conclusion:

As a conclusion we have made an approach by which we can do Image Authentication based on Histogram Shifting Method using Arnold's Cat Map. Get good result for without attack. But get some dilute result on with attack.

We can use this method if there is no such attacks then our algorithm is fine for the image hiding technique

References:

1. Reversible data hiding exploiting spatial correlation between sub-sampled images Kyung-Su Kima,∗, Min-Jeong Leea, Hae-Yeoun Leeb, Heung-Kyu Leea
2. Applying Reversible Data Hiding for Medical Images in Hybrid Domain Using Haar and Modified Histogram Vanmathi Chandrasekaran1* Prabu Sevugan2
3. Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking Hiba Abdel-Nabi and Ali Al-Haj Department of Computer Engineering Princess Sumaya University for Technology Amman, Jordan
4. High Capacity Reversible Data hiding based on histogram shifting for Medical Images C. Vinoth Kumar, V. Natarajan and Deepika Bhogad
5. Secure Reversible Data Hiding in the Medical Image using Histogram Shifting and RC4 Encryption De Rosal Ignatius Moses Setiadi Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia moses@dsn.dinus.ac.id Md Kamruzzaman Sarker Department of Computer Science and Engineering Wright State University Dayton, United States sarker.3@wright.edu Muhammad Fadhil Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia mfadhil70@gmail.com Pulung Nurtantio Andono Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia pulung@research.dinus.ac.id Eko Hari Rachmawanto Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia eko.hari@dsn.dinus.ac.id Ifan Rizqa Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia risqa.ifan@dsn.dinus.ac.id Christy Atika Sari Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia atika.sari@dsn.dinus.ac.id Andik Setyono Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia andik.setyono@dsn.dinus.ac.id
6. A reversible data hiding method by histogram shifting in high quality medical images Li-Chin Huangc, Lin-Yu Tseng b, Min-Shiang Hwanga,∗
7. Reversible Image Hiding for High Image Quality based on Histogram Shifting and Local Complexity Chin-Chen Chang1,2 , Thai-Son Nguyen1,4 , and Chia-Chen Lin3
8. Medical image steganographic algorithm via modified LSB method and chaotic map A. A. Karawia
9. Reversible data hiding exploiting spatial correlation between sub-sampled images Kyung-Su Kima,∗, Min-Jeong Leea, Hae-Yeoun Leeb, Heung-Kyu Leea

10. B. Li, J. He, J. Huang, Y. Q. Shi, “A Survey on Image Steganography and Steganalysis”, Journal of Information Hiding and Multimedia Signal Processing., Vol. 2, Issue 2, pp.142-172. (2011).

11. T. Lu and T. N. Vo, "Digital Media Steganography, Principles, Algorithms, and Advances”, Academic Press, Egypt, pp.189-213, ISBN. 9780128194386. (2020)
12. J.R. Krenn, “Steganography and Steganalysis”. (2004)
13. A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, “Digital image steganography: Survey and analysis of current methods”, Volume 90, Issue 3, Pages 727-752. (2010)
14. F.Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press. (2017)
15. I. J. Kadhim, P. Prashan, P. J. Vial, B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research”, Neurocomputing, Volume 335, Issue C, pp 299–326, https://doi.org/10.1016/j.neucom.2018.06.075. (2019)
16. H. Wang, S. Wang, “Cyber warfare: steganography vs. steganalysis” Communications of the ACM, Volume 47, Issue 10, pp 76–82. (2004)
17. H. Mathkour, B. Al-Sadoon, and A. Touir, "A New Image Steganography Technique," 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, pp. 1-4, doi: 10.1109/WiCom.2008.2918. (2008)
18. A. A. J. Altaay, S. B. Sahib and M. Zamani, "An Introduction to Image Steganography Techniques," 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 2012, pp. 122-126, doi: 10.1109/ACSAT.2012.25. (2012)

19. VenkatramanS, Ajith Abraham and M. Paprzycki, "Significance of steganography on data security," International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., Las Vegas, NV, USA, pp. 347-351 Vol.2, doi: 10.1109/ITCC.2004.1286660. (2004)
20. H. Daren, L. Jiufen, H. Jiwu, and L. Hongmei, "A DWT-based image watermarking algorithm," IEEE International Conference on Multimedia and Expo, ICME 2001., Tokyo, Japan, 2001, pp. 313-316, doi: 10.1109/ICME.2001.1237719. (2001)
21. A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques," 2016 International Conference on Research Advances

in Integrated Navigation Systems (RAINS), Bangalore, India, pp. 1-8, doi: 10.1109/RAINS.2016.7764399. (2016)

22. S. Kalman, D. Zheng, J. Zhao, W. J. Tam, and F. Speranza, "An Image Quality Evaluation Method Based on Digital Watermarking," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 1, pp. 98-105, doi: 10.1109/TCSVT.2006.887086. (2007)

23. J. C. Lee, “Analysis of attacks on common watermarking technique.” IEEE Electrical and Computer Engineering Department University of British Columbia 2Anand6 Main Mall, Vancouver, BC Canada V6T 1Z4.

24. R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," in IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128, doi: 10.1109/6046.985560. (2002)

25. Kumari, M.R.R., Kumar, V.V. & Naidu, K.R., “Digital image watermarking using DWT-SVD with enhanced tunicate swarm optimization algorithm.” Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-14618-4

26. S. Sattarpour, “Robust optimal image watermarking using graph-based and discrete wavelet transforms, and whale optimization algorithm.” Multimed Tools Appl 82, 6667–6685 (2023). https://doi.org/10.1007/s11042-022-13639-9

27. P. Garg, A. Jain, “A robust technique for biometric image authentication using invisible watermarking.” Multimed Tools Appl 82, 2237–2253 (2023). https://doi.org/10.1007/s11042-022-13314-z

28. A. G. Weber, “The USC-SIPI Image Database: Version 6”, Ming Hsieh Department of Electrical Engineering Signal and Image Processing Institute. (2018)

29. https://dde.binghamton.edu/download/https://www.kaggle.com/datasets/kmader/siim-medical-images