

IMAGE AUTHENTICATION AND TAMPERED DETECTION USING STEGANOGRAPHY APPROACH

Sudipta Roy¹, Anushka Gupta² and Arindam Goswami³

¹ BPPIMT , Kolkata , India

² Information Technology , BPPIMT , Kolkata , India

³ Information Technology , BPPIMT , Kolkata , India

Abstract. The validity of digital photos has recently come into doubt due to the quick development of digital image altering technologies. A system called picture tampering detection uses the inherent image regularities to identify manipulated photographs. Existing intrinsic image regularities, however, are made for a certain class of tampering procedures. picture tampering detection accuracy is significantly reduced when many types of tampering activities are utilised to manipulate a digital picture. The re-normalized histogram of noise and noise difference, which is calculated as the histogram to peak-value ratio, is used in this study to identify a new class of intrinsic picture regularities. The re-normalized histogram would rise when the peak value of this histogram fell when the image was altered through image tampering. Making use of the re-normalized the experimental findings demonstrate that the suggested technique can detect a variety of tamper activities, including single type and many kinds of tamper operations, without knowing the tampering operation sequence, type, or parameter beforehand.

Keywords: Spatial domain, PSNR, steganography , tampering

I. INTRODUCTION— In the field of digital image processing, ensuring the security and integrity of images has become increasingly important. One approach to address this concern is the embedding of a secret image within a cover image using techniques such as Discrete Cosine Transform (DCT) and Pseudo-Noise (PN) sequences. This research focuses on the process of embedding a 32x32 bitmap (.bmp) image into a 512x512 cover image, as well as the subsequent extraction process involving tampering detection and noise analysis.

In addition to the embedding and extraction processes, this report also focuses on tampering detection and noise analysis. Tampering detection is achieved by introducing intentional modifications to the watermarked image during transmission, simulating potential attacks or alterations. Incorporating noise into the image during tampering further enhances the realism of the analysis. At the receiver's end, the tampered image with integrated noise is processed to extract the watermark image. By tracking the differences between the original and extracted watermark images, evaluating the average values of sub-block elements, and comparing them with predefined threshold values, the distortion and tampering effects on the extracted watermark image can be assessed. Through a comprehensive analysis of the quantified values obtained from the tampering detection and noise analysis processes, this report aims to provide insights into the distortion and tampering scenarios in the extracted watermark image. This information can contribute to the development of robust

techniques for secure image embedding, extraction, and tampering detection, ensuring the integrity and authenticity of digital images in various applications

Why we need Data Security?

Data protection from hackers and other invaders requires security. Cryptography is one of the most crucial techniques for maintaining data privacy. Writing in secret is known as cryptography, and it protects data security. Data that is well-hidden cannot be easily accessed, altered, or created. Important data is protected via cryptography by being transformed into ambiguous data that can only be read by authorised receivers, who then translate the ambiguous data back into the original language. With the use of a specific key, the act of converting plaintext into obscure text (ciphertext) is known as encryption, and the reverse is known as decryption. Spatial or picture domain and frequency or transform domain are the two primary categories into which the steganography algorithm may be divided. By directly manipulating the pixel values in the frequency or transform domain, secret message bits may be added to the coefficients, whereas in the spatial domain, secret message bits are added to the cover picture by directly manipulating the pixel values. The pros and drawbacks of each category are different. While frequency domain algorithms are more durable and less prone to assaults, they have a lower capacity and are more susceptible to statistical, compression, and cropping attacks. A few examples of stego attacks are picture resizing, image manipulation.

II. Cryptography

A technique for maintaining message secrecy is cryptography. The term has a specific meaning in Greek, which is "hidden writing." Nowadays, however, high-level cryptography is used to preserve people's and organisations' privacy, ensuring that information is transferred securely and that only the intended recipient has access to it. With historical roots, cryptography is a conventional technique that is still being researched. Instances date as far back as 2000 B.C., when the ancient Egyptians employed "secret" hieroglyphics. There is also more proof in the shape of coded texts from ancient Greece and Rome, including the well-known Caesar cipher. While the majority of people are unaware of it, hundreds of millions of individuals regularly utilise encryption to secure data and information. In addition to being incredibly beneficial, cryptographic systems also quite vulnerable to compromise from a single programming or specification error.[14]

Secure communication channels are the goal of cryptography. It offers data encryption methods so that only the holder of the decryption key may unlock the message's encryption. It has the advantage of prohibiting any updates or modifications made to the communication channel by an attacker. A public-key cipher and hash algorithms are used to achieve this. A maximum level of privacy is guaranteed by the majority of cryptographic methods, including RSA, Blowfish, DES, and AES. Maximum security is also achieved by the hybridization of these techniques. Despite the fact that these methods are crucial for encrypting text data, they are ineffective for picture security due to the fact that images include crucial characteristics like multiple redundancies and a strong connection between nearby pixels. Image security must thus be achieved effectively.

II.I Cryptography Types

Three major kinds of cryptography exist. These are listed below:

1. **Symmetric key encryption:** It uses the same key for encryption and decoding, takes less time to perform, and uses a key to encode and decode both normal text and cipher text.

2. **Asymmetric key encryption:** Two keys are used in the public key encryption method: a secret key and a public key. To secure the communication, the sender receives the recipient's public key. The recipient, on the other hand, makes use of the secret key to decrypt the communication. The passwords can be used by different organisations.
3. **Hashing Operations:** Another kind of cryptography device is a hash algorithm. The random input values are used, and a set output value is generated that can be used to identify the person and retrieve private information. These features are used to secure credentials by many OS.[15]

A. Typical Cryptography Terminology

- Plaintext:** The authentic and comprehensible text. For instance, "Y" needs to send "Z" a "Computer" message. In this case, "Computer" refers to the plaintext or first message.
- Ciphertext:** The string "A@\$&J9," is written in a way that no one can decipher it.
- Encryption:** The conversion of plain text into obscure text. A key and an encipherment algorithm are required for the method of encoding. On the sender's end, encipherment takes place.
- Decryption:** It is the opposite of encryption. It is a technique for turning plaintext into ciphertext.
- Key:** A key might be a special character, a number, or both. It is applied both to the source text during encipherment and to the ciphertext during decoding.

III. Steganography

Steganography, which means "concealed writing," give rise to the term. The word "write" is graphein. The phrase was originally used by Johannes Trithemius in his *Steganographia*, a dissertation on steganography and encryption that was published as a book on magic in 1499. Messages typically seem to be something else, such as pictures, articles, shopping lists, or other cover material. In the past, a concealed message would have been written in invisible ink between the lines that can be seen on a private letter. "Steganography" fills a need in security by enhancing cryptography rather than substituting it. Another degree of security is added if a secret message is encrypted and must be decoded upon discovery. Several methods of steganographic classification exist. Depending on the context, the carrier files may be referred to as cover text, cover picture, or cover audio. The purpose of the steganography is to prevent suspicion being raised about the existence of the information rather than to prevent others from discovering the hidden information. A steganography technique fails if it leads someone to believe that a carrier media contains hidden information. The Herodotus narrative about slaves with shaved heads is the earliest literary instance of steganography being used to transmit. The most current illustration of steganography is provided in terms of the issue facing the prisoner.

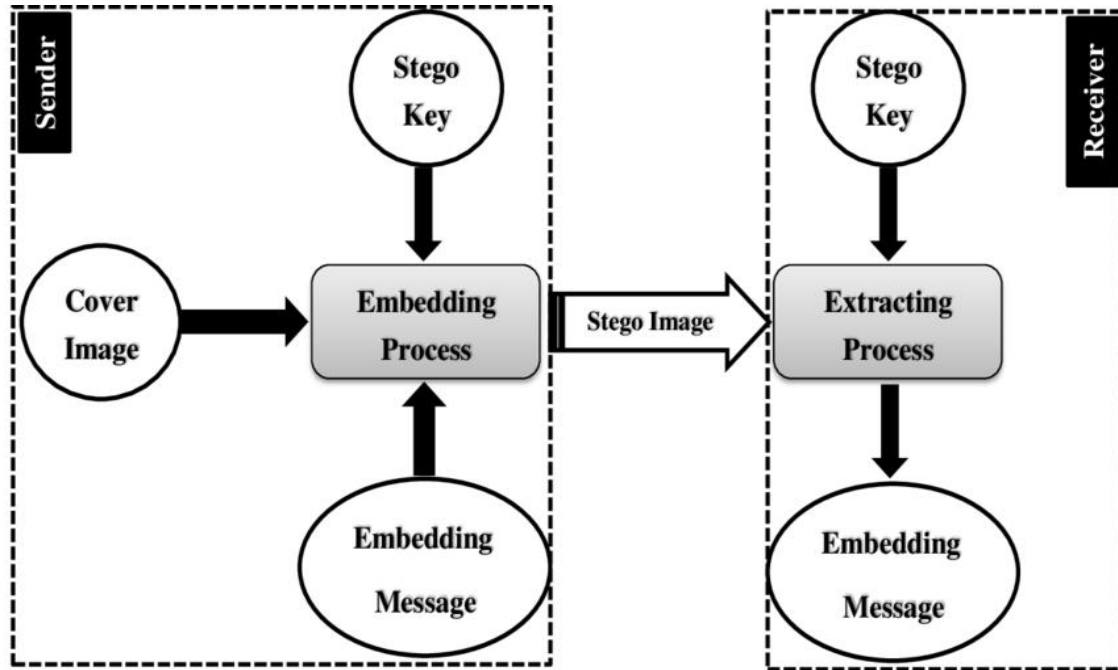


Figure 1: A Steganography Framework

In steganography, the cover carriers that might carry the secret information include pictures, audio, video, and text. A message, which can be plaintext, cipher text, pictures, or anything else that can be incorporated into a bit stream, contains the information that is concealed. A stego-carrier is made of the cover carrier and the embedded message. A stego-key, which is extra secret information, like a password, necessary for embedding the information, may be needed to hide information. A stego-image is created, for instance, when a secret message is concealed behind a cover picture. The formula might be written as follows:

$$\text{Cover medium} + \text{Embedded message} + \text{Stego key} = \text{Stego medium.}$$

III.I Forms of Steganography

Different types of steganography exist. The following are a few of the forms:

1. Audio steganography: Encoding a hidden message into an audio signal is helpful because it modifies the binary order of the corresponding audio file. Digital sound steganography is a more intricate form of steganography than other steganography.

2. Image steganography: Picture steganography is the method of obscuring information by using the cover object as the picture. Given the largenumber of bits used in an image's digital depiction, it is a common cover source in digital steganography. Information can be hidden in a picture in a variety of ways. The following are these techniques: Coding with the least significant bits Cosine transformation, Filtering, Masking Encryption of Redundant Pattern Encoding

3. Video Steganography: Because video steganography mixes sound and picture, it provides more possibilities for masking large amounts of data. The movie may therefore incorporate both picture and audio steganography methods.

4. Text Steganography: It includes text files that hide info. With this method, each text message word's nth character conceals the hidden data underneath. There are many ways to conceal information in text files.

5. Networks or protocol steganography: By using network protocols like TCP, UDP, ICMP, and IP as cover objects, it entails hiding information. The OSI layer network architecture has covert routes that can be utilised with steganography.[5]

III.II. LSB Steganography

The least significant bit (LSB) replacement technique is the most straightforward and well-liked picture steganography technique. By altering the least important elements of the cover picture directly, the messages are inserted using this technique. Using up to 4 least significant bits in each pixel, which is likewise very difficult to detect, increases the concealing capacity.

Steganography methods on LSB

A. Stego One Bit

Only one LSB of the pixel is altered by this technique. Just one will be added or subtracted from the LSB's integer value. It's hard to notice this minor modification. This is the first technique to be tested, and it will entail encoding some of the fundamental steps needed to test other Steganographic techniques as well. This should have a negligibly little impact on the image's look.

B. Stego Two Bit

With this technique, the message bits in the picture will be stored in the image using two LSBs of one of the colours in the RGB value of the pixels. The image will be more deformed, but the data concealing capability is four times that of stego 1 bit.

C. Stego Three Bit

The message bits will be stored using this technique using three LSBs of one of the colours in the RGB value of the pixels. While the image would be significantly more distorted, the data concealing capability is three times that of Stego One Bit.

D. High Capacity Pixel Indicator Technology

To signal the presence of data on the other two channels, it employs the least two significant bits of one of the channels.

Indicator values for the pixel indicator approach are explained in Table 1.

E. Triple-A: Randomization-based

Encryption and hiding are the two main components of this technique.

1) Encryption: Section one deals with utilising the AES method to encrypt the message (M), which will result in Enc (M, K). In practise, a collection of user passwords may be used to produce the key K.[5]

2) Hiding: A cover medium called the RGB Picture is utilised.

According to the triple-A approach, which requires a pseudorandom number generator, Enc (M, K) is concealed (PRNG).

Every iteration of the PRNG is supposed to provide two fresh random numbers. The Key determines how these PRNGs' Seed1 (S1) and Seed2 (S2) seeds are created (K). S1 can only produce numbers between . The RGB image's component that will be utilised to conceal the encrypted data Enc is chosen using the S1 random number (M, K). Table 2 demonstrates how the (S1) random number chooses the RGB elements. S2 is only applicable to the range . The amount of least significant bits utilised to conceal the secret data is chosen using the S2 random number. Table 3 demonstrates how the (S2) random number influences the total amount of bits. Combining information from the earlier tables, we can observe that each pixel uses a minimum of 1 bit. If we just use one bit of the RGB image's selected component

III.III MSB Steganography

The LSB steganography has been somewhat modified by this technique. The most significant bit is modified in this manner instead of the least important bit. In this instance, the embedded value is kept in the image's most important bits.

III.IV RGB Steganography

An array of values that indicate the light intensities at various spots or pixels make up a digital picture. The two most common file formats for digital computer images are 24-bit (RGB) and 8-bit (Grayscale). Although a 24-bit file might be rather big, it offers greater room for information concealment. As is common knowledge, red, green, and blue are the three fundamental colours that make up all hues. Every basic colour is represented by one byte, therefore each pixel is a mixture of all the fundamental colours (R,G,B).

STEGANOGRAPHIC SYSTEM NEEDS

Imperceptibility: Both the stego image and the original picture, should be similar in perception. Invisibly inserted data.

Robustness: The embedded data should be as large as possible and robust enough to withstand multiple attacks.

Increasing embedded data capacity while maintaining security. Uses and Significance of a Steganographic System as a Security Reinforcement Layer for Cryptography. It is utilised in the fields of military, business, education, and digital watermarks and fingerprinting. Image using the restricted capabilities of the human visual system is the goal of steganography (HVS). Any text that can be contained in a bit stream, including plain text, encrypted text, other pictures, and other data, may theoretically be concealed in an image. Image with the advent of fast, potent graphical computers, steganography has advanced quite a bit recently.

TECHNIQUES FOR IMAGE STEGANOGRAPHY

A. Steganography based on the spatial domain

It uses LSB (Least Significant Bit) steganography. Due to their excellent concealment, enormous capacity for concealed information, and simplicity of realisation, spatial approaches are most commonly used. Sequential Embedding and Scattered Embedding are two LSB Steganography techniques.

B. Transform Domain Based Steganography

Transform domain Steganography involves hiding information by encoding it in the transform coefficients.

C. Document-based Steganography

By inserting tabs or spaces into .txt or .doc files, this technique embeds data in documents.

D. File Structure-Based Steganography

With this technique, hidden data is inserted into the unnecessary parts of cover files, such as the reserved bits in the file header or the marker segments in the file format.

EMBEDDING OF SPATIAL DOMAIN

By substituting the message to be conveyed for the LSB of the pixels in the LSB approach, bits are distributed equally, resulting in an average of just half of the LSBs being updated.

Most Minimal Significant Bit Method, think of a 24-bit image.

Character 'A' in the data to be entered: (10000011)

In order to store one 8-bit character, 3 pixels will be utilised.

Example:

```
00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001
```

Embedding 'A'

```
00100111 11101000 11001000
00100110 11001000 11101000
11001001 00100111 11101001
```

IV. Performance metrics (MSE, PSNR, SSI, CC)

These metrics provide different perspectives on the performance or quality of processed data, and their interpretation depends on the specific application and context.

Mean Squared Error (MSE): MSE is a measure of the average squared difference between the original and reconstructed (or denoised) data. It is widely used to quantify the overall distortion or error between two signals or images. The lower the MSE, the better the performance, as it indicates less deviation between the original and processed data.

Peak Signal-to-Noise Ratio (PSNR): PSNR is a metric that measures the ratio between the maximum possible power of a signal (or image) and the power of the noise that affects it. It is commonly used to evaluate the quality of reconstructed or compressed images by comparing them to the original image. Higher PSNR values indicate better quality, as it signifies a higher signal-to-noise ratio.

$$\text{PSNR} = 10 \cdot \log(P_2 / \text{MSE})$$

Cross-Correlation (CC): Cross-correlation is a measure of similarity between two signals or images. It quantifies how much two signals correlate or resemble each other. In image processing, it is often used to assess the alignment or matching of two images. A higher CC value indicates a stronger similarity or correlation between the two signals.

Structural Similarity Index (SSI): The Structural Similarity Index (SSI), also known as SSIM, is a metric that measures the perceived similarity between two images. It considers the structural information, luminance, and contrast of the images. SSI is designed to capture aspects of human visual perception and is widely used in image and video processing applications. A higher SSI value indicates a higher similarity or perceived quality between the images.

V. Comparison between steganography and cryptography:

Cryptography and steganography are crucial components of network security. Network security has developed into a crucial part of the information architecture of the present. Network security was essential for maintaining data accuracy and secrecy. It guards against unauthorised entry for the individual. Steganography hides contact tracks, whereas cryptography encrypts the message to make it unintelligible.

V.I Cryptanalysis issues

Cryptography has the following issues:

- 1) Problems with key distribution
- 2) Problems with key distribution
- 3) Cryptanalysis

VI. Digital Image watermarking

Secure communication channels are the goal of cryptography. It offers data encryption methods so that only the holder of the decryption key may unlock the message's encryption. It has the advantage of prohibiting any updates or modifications made to the communication channel by an attacker. A public-key cipher and hash algorithms are used to achieve this. A maximum level of privacy is guaranteed by the majority of cryptographic methods, including RSA, Blowfish, DES, and AES. Maximum security is also achieved by the hybridization of these techniques. Despite the fact that these methods are crucial for encrypting text data, they are ineffective for picture security due to the fact that images include crucial characteristics like multiple redundancies and a strong connection between nearby pixels. Image security must thus be achieved effectively.

TYPES OF WATERMARKING:

Visible Watermarking: Visible watermarking involves embedding visible information or logos onto an image or video. These watermarks are easily noticeable and serve as a form of copyright protection or branding. They are typically added in a semi-transparent manner, allowing the underlying content to remain visible. Visible watermarks are commonly used in digital media to deter unauthorized usage or redistribution.

Invisible Watermarking: Invisible watermarking, also known as digital or imperceptible watermarking, involves embedding a watermark that is not visually apparent in the content. The watermark is imperceptible to human observers, but it can be detected and extracted using appropriate techniques. Invisible watermarks are primarily used for copyright protection, content authentication, and tamper detection.

Spatial Domain Watermarking: Spatial domain watermarking refers to the embedding of the watermark directly into the spatial domain of the host image or video. The watermark bits are typically embedded by modifying the pixel values or the least significant bits (LSBs) of the image. Spatial domain techniques are simple and computationally efficient but can be vulnerable to attacks such as image cropping or resizing.

Frequency Domain Watermarking: Frequency domain watermarking involves embedding the watermark in the frequency domain of the host image or video. Commonly used techniques include Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT). Frequency domain watermarking provides

robustness against common signal processing operations and offers better resistance to attacks compared to spatial domain techniques.

Spread Spectrum Watermarking: Spread Spectrum watermarking techniques involve spreading the watermark information across the entire host signal using a pseudo random (PN) noise sequence. This approach provides robustness against attacks and ensures that the watermark remains detectable even if parts of the host signal are altered or removed. Spread Spectrum watermarking is commonly used in audio and image watermarking applications.

TYPES OF TRANSFORMATION DOMAIN:

Discrete Cosine Transform (DCT): DCT is a widely employed transform domain for watermarking applications. It converts the spatial domain representation of an image into frequency domain coefficients. The DCT coefficients capture the image's energy distribution and are suitable for embedding watermarks due to their energy compaction properties. DCT-based watermarking techniques offer good robustness against common attacks such as compression and filtering.

Discrete Wavelet Transform (DWT): DWT is a versatile transform domain that provides both spatial and frequency localization. It decomposes an image into different frequency subbands, capturing both high-frequency details and low-frequency components. Watermarking in the DWT domain enables embedding the watermark selectively in specific subbands, providing robustness against various signal processing operations. DWT-based techniques are well suited for scalable and robust watermarking applications.

Discrete Fourier Transform (DFT): DFT is a transform domain that converts an image from the spatial domain to the frequency domain. It represents the image using complex numbers, where the magnitude and phase spectra carry important frequency information. DFT-based watermarking techniques exploit the frequency components of the image to embed and extract watermarks. They are commonly used in audio and speech watermarking applications.

Discrete Radon Transform (DRT): DRT is a transform domain used for watermarking applications, particularly in medical imaging. It is based on the Radon transform, which captures the image's line integrals or projections from different angles. Watermark embedding and extraction in the DRT domain involve modifying the projection data to embed and retrieve the watermark information.

Singular Value Decomposition (SVD): SVD is a matrix decomposition technique used for watermarking applications, primarily in image and video watermarking. It decomposes an image or video into three matrices: the left singular vectors, singular values, and right singular vectors. Watermark embedding and extraction in the SVD domain involve modifying the singular values to embed and retrieve the watermark. SVD-based watermarking techniques offer good robustness against geometric transformations and compression.

VII. Image tampering

Due to the availability of strong instruments in the area of editing and changing these media, digital media like digital pictures and papers should be authenticated against forgery. Digital photography has developed into the industry standard for producing, editing, and archiving visual memories and proof. Although this technology has many benefits, it can also be used as a deceptive instrument to conceal facts and proof. This is so that forgery cannot be seen physically due to the precision with which modern digital pictures can be altered. In reality, the security of digital content has long been a worry, and numerous methods for confirming the reliability of digital images have been created. In disciplines like

investigations and medical imaging. Digital picture integrity and veracity are crucial for e-commerce and industrial photos has been mentioned in a detailing manner in [2] by Minati mishra. Imaging is used by doctors and experts in the medical industry to make diagnoses. Truth, deception, and the purity of digital pictures are ethical problems that are brought up by the introduction and quick spread of digital manipulation to still and moving images. Professionals pushing the ethical limits of truth raises the possibility of the public losing faith in digital media. This necessitates the development of monitoring tools that are impervious to manipulation and can determine whether an image has been altered simply by looking at the altered image.

A. Active Tamper Detection Techniques: Despite being less prevalent than passive techniques due to their intrinsic limitations, active taper detection techniques are still thought to be the most effective methods for picture authentication, and extensive research has been conducted in this area. These active picture authentication methods are typically divided into two groups: the first one employs a delicate watermark that can identify and locate content changes. Although these techniques have a very high rate of tamper detection, they cannot tell the difference between basic brightness and contrast changes and the substitution or addition of scene components. Even though the picture is intact, increasing the gray scales of all pixels by one would suggest extensive manipulation. A number of researchers worked on these active tamper detection and authentication schemes and created a variety of fragile, semi-fragile, robust, public as well as private key based watermarks for copyright protection, authentication, and tamper detection. Some of these failed to solve the issues or sacrificed the accuracy of the original methods' tamper localization, but a select few were found to be highly effective and efficient. However, the hierarchical digital watermarking method put forth by Phen et al. is a straightforward but effective method that not only locates and discovers manipulation but also has the ability to recoup from tampering with a minimal loss in picture quality. After level-2 and level-3 examination, this method's accuracy in tamper discovery and location is 99.6% and 100%, respectively. For a picture that has been altered by less than 50%, the counterfeit recovery rate is higher than 93%[2].

B. Passive Tamper Detection Techniques: The inactive techniques are thought of as advancements in tamper detection progression. These methods don't require any previous knowledge of the picture or the pre-embedding of any watermark or digital identity into the image, in opposition to active authentication techniques.

Cloning Detection - one of the most popular methods of image manipulation is to clone or duplicate and paste a portion of the picture to hide an object or individual. When done carefully, it becomes nearly impossible to see the clone, and since the cloned area can be of any shape or size and be situated anywhere in the image, it is practically difficult to perform a thorough scan of all sizes to all potential image locations. Any Copy-Move forgery, according to , establishes a correlation between the original picture section and the pasted one that can be used as a foundation for effective identification of this kind of forging. The portions might only match roughly rather than precisely because the altered picture will probably be reduced and because smoothing or other post-processing techniques may be used. In this article, the authors present two distinct detection strategies: exact and robust matching, which can identify identical areas in an image even after the images have undergone post-processing as a result of copy-and-paste. For the stable identification of copied areas in an image, methods based on blur movement invariants and DWT, SVD, and PCA-based sorted neighbourhood techniques are proposed in . [2]

Splicing Detection - Techniques for Splicing Detection Another frequently used image manipulation method is digitally combining two or more pictures into a single image. When done correctly, the boundaries between the spliced areas may be invisible to the human eye. It is a common technique to manipulate an image's semantic content in order to lead the observer to think something other than what is actually happening. An essential step in image forgery, image splicing is characterised by a straightforward cut-and-paste operation that involves taking a portion of an image and pasting it onto the same or a different image without applying any post-processing smoothing, such as edge blurring or

blending. Image hacking typically refers to splicing followed by post-processing steps to render the alteration invisible to the human eye[2].

VIII TYPES OF IMAGE TAMPERING TECHNIQUES

Image manipulation is a form of digital art that requires a grasp of image characteristics as well as strong visual imagination. Images can be altered for a variety of reasons, such as for entertainment purposes when using digital tools to create amazing photographs or to create false proof. Whatever the reason for the deed, the forger should employ a single image processing procedure or a combination of several.

The following are the numerous methods of altering images that are frequently used.

a)**Copy-move** : The most popular method of altering images is called copy-move, which requires covering a portion of the picture in order to add or delete information. Used as the best sections for copy-move forgery are textured areas. Due to their comparable hue, dynamic range, and noise variation characteristics, textured regions in the picture, it won't be visible to the human eye when looking for inconsistencies in the statistical characteristics of the image.

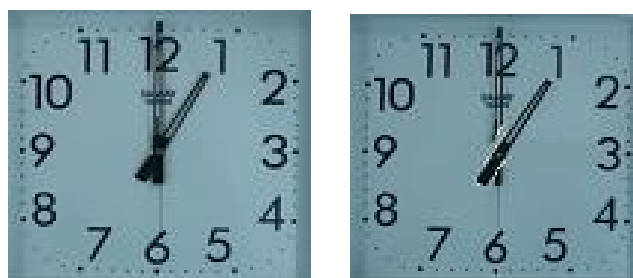


Figure 2 : Copy- Move Forgery

b)**Image-splicing** : It is the process of pasting together digital pictures to create a paste-up. While the act of making composite photographs dates back to the creation of cameras, the word "photomontage" was first used to describe an artistic style. Although the act of making composite photographs dates back to the creation of cameras, the word "photomontage" was first used to allude to an artistic style.

c)**Resize**: It is a geometric procedure that can be used to change the size of a picture or a portion of an image. By interpolating between pixel values in nearby neighborhoods, image compression is accomplished. By converting between neighbouring pixel values, image compression is accomplished.

d)**Cropping**: It is a technique to cut-off borders of an image or reduces the canvas on which an image is displayed. Generally this kind of operation is used to remove border information which is not very important for display.

e) **Noising or Blurring**: A spectator can clearly see the results of image manipulation operations like image splicing, scaling, and turning in the form of artefacts like incorrect borders, aliasing flaws, and tone variations. Applying a small quantity of noise or blur operations to the areas where the tampering flaws are visible will mask these apparent signs of tampering.

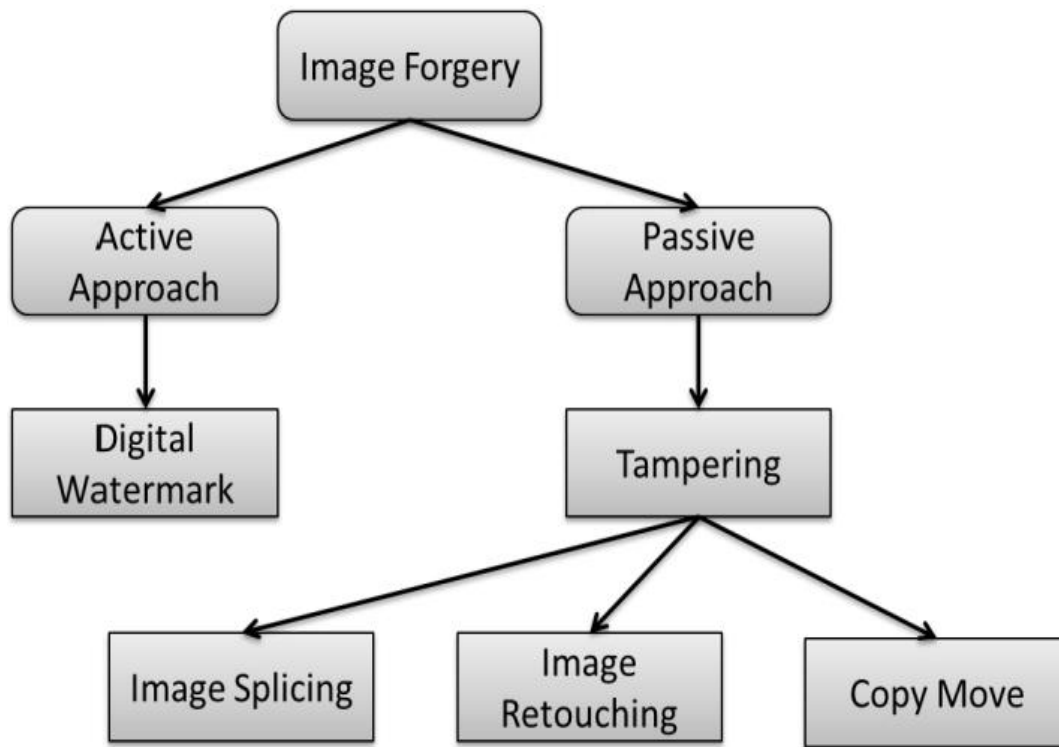


Fig 3 : Types of Image Forgery

Noise

In the context of tampering detection, noise refers to any unwanted or undesired variation or interference in the signal or data being analyzed. Tampering detection systems are designed to identify unauthorized modifications or alterations to a system, such as tampering with hardware components or modifying software code.

Different types of noise can occur in tampering detection, including:

Salt and Pepper Noise : In the context of image tampering detection, salt and pepper noise can be intentionally added to an image to conceal or manipulate certain parts of the content. By introducing this noise, an attacker may try to make it more difficult for automated algorithms or human observers to detect the tampering.



Watermarked Image


 Tampered Image using salt and pepper noise (0.10%)
 Fig 4(a)

Gaussian Noise: Gaussian noise, also known as white noise, is a type of random noise that follows a Gaussian distribution. It is characterized by its constant power spectral density, meaning it has equal energy at all frequencies. Gaussian noise is statistically uncorrelated, and each sample is independent of the others. It is often used as a reference for analyzing the impact of noise on a system or for simulating random disturbances.



Fig 4(b)

Fig 4(a) and (b): Tampering an watermarked image using different noises

Applications

Tampering detection has several applications across various domains. Here are some common areas where tampering Detection systems are used:

Physical Security Systems: Tampering detection is widely used in physical security systems, such as alarm systems, access control systems, and surveillance systems. These systems employ sensors, cameras, motion detectors, or vibration detectors to detect any unauthorized tampering with doors, windows, security devices, or sensitive areas.

Anti-Tamper Technologies: Tampering detection plays a crucial role in anti-tamper technologies used to protect sensitive or valuable assets. For example, in the defense industry, tamper-resistant packaging, seals, or devices are used to detect any attempts to open, modify, or tamper with critical equipment, weapon systems, or communication devices.

Data Integrity and Authentication: In digital systems, tampering detection is essential for ensuring the integrity and authenticity of data. Cryptographic techniques, digital signatures, and checksums are used to detect any modifications or unauthorized changes in data during storage, transmission, or processing. This is crucial in areas such as financial transactions, electronic voting systems, or secure communication protocols.

Software and Firmware Protection: Tampering detection is used to safeguard software applications and firmware from unauthorized modifications or reverse engineering. Techniques such as code obfuscation, checksum verification, or code integrity checks help detect and prevent tampering attempts, ensuring the integrity and security of the software or firmware.

Proposed Algorithm:

In this Project, the proposed algorithm focuses on embedding a 32x32 bitmap (.bmp) image into a 512x512 cover image using Discrete Cosine Transform (DCT) and Pseudo-Noise (PN) sequence. The goal is to achieve secure watermarking and develop tampering detection mechanisms along with noise analysis.

The embedding process starts by converting the original RGB image to the YCbCr color space, where the Y channel is extracted for watermark embedding. A PN sequence is generated using a security key to ensure secure embedding. The Y-channel is permuted using the PN sequence, and then divided into non-overlapping 8x8 blocks. DCT is applied to each block, and 1024 randomly selected blocks are used to embed the watermark pixels with a strength of 0.1. Inverse DCT (IDCT) is applied to each block, and the blocks are combined to reconstruct the original dimensions. The permutation is then removed, and the RGB channels are combined to form the watermarked image.

For extraction, the algorithm retrieves the Y-channel, applies DCT to 8x8 blocks, and calculates the difference at the pixel locations where the watermark is embedded. Positive differences correspond to background pixels, while negative differences correspond to foreground pixels of the watermark.

The tampering detection process involves several steps. First, the original cover image is inputted at the client side. The watermark image is hidden in the cover image using DCT and the PN sequence. Tampering is then applied to the stego image during transmission, incorporating noise. At the receiver's end, the tampered image is received, and the watermark image is extracted from the stego image.

To detect tampering and distortion in the extracted watermark image, several analysis techniques are applied. The differences between similar color pixel byte elements within specific sub-block images of the original and extracted watermarks are tracked. Ratios of counter variables related to these differences are computed based on a specific threshold value. The average values of all sub-block elements in the concerned sub-block images are also computed, and ratios of counter variables related to these average differences are evaluated. Additionally, the similarity aspect between the original and extracted watermark images is analyzed based on standard parameters. By comparing the quantified values and threshold values, the distortion and tampering effects on the extracted watermark image can be determined.

Overall, the proposed work aims to embed a bitmap image into a cover image using DCT and PN sequence, while also incorporating tampering detection mechanisms and noise analysis. The tampering detection process involves tracking differences, computing ratios, and evaluating distortion scenarios in the extracted watermark image.

Embedded Algorithm:

The provided code implements a blind watermarking algorithm using the Discrete Cosine Transform (DCT). The algorithm takes an original image 'x', a watermark image, and a key as input, and it returns a watermarked image 'y'.

Here is a step-by-step explanation of the algorithm:

1. Convert the original image 'x' from the RGB color space to the YCbCr color space using the 'rgb2ycbcr' function.
2. Extract the individual channels (Y, Cb, and Cr) from the YCbCr image.
3. Generate a pseudo-random noise (PN) sequence for permutation. The key is used to initialize the random number generator ('rng') to ensure reproducibility.
4. Perform permutation on the Y channel of the image. Each pixel in the Y channel is permuted based on the PN sequence as follows:
 - If the corresponding PN value is 1, the pixel value is replaced with the product of the PN value and the current pixel value, and the pixel value at the corresponding position (j, i) is replaced with the complement of the PN value multiplied by the pixel value at position (i, j).
 - If the PN value is 0, the pixel value remains unchanged.

5. Resize the watermark image to a target size (32x32) while maintaining the aspect ratio using the 'imresize' function.
6. Convert the resized watermark image to binary using the 'imbinarize' function.
7. Reshape the binary watermark image into a vector ('W_vec') by concatenating its columns.
8. Divide the permuted Y channel into 8x8 blocks and apply the DCT (Discrete Cosine Transform) to each block. The resulting DCT coefficients are stored in the 'blocks' cell array.
9. Select a random set of blocks from the 'blocks' array to embed the watermark. The selection is based on the key provided. The number of selected blocks is equal to the number of elements in the watermark vector.
10. Perform the embedding stage by modifying the DCT coefficient at the position (4, 2) in each selected block. If the corresponding watermark bit is 0, decrease the DCT coefficient by a small value ('alpha'). If the watermark bit is 1, increase the DCT coefficient by 'alpha'.
11. Combine the modified blocks back to their original dimensions and apply the inverse DCT (IDCT) to each block. The resulting blocks form the watermarked Y channel ('Y_watermarked').
12. Reverse the permutation applied in 'step 4' to retrieve the original Y channel. Each pixel in the Y channel is reversed according to the PN sequence as follows:
 - If the corresponding PN value is 1, the pixel value is replaced with the product of the PN value and the original pixel value, and the pixel value at the corresponding position (j, i) is replaced with the complement of the PN value multiplied by the watermarked pixel value at position (i, j).
 - If the PN value is 0, the pixel value remains unchanged.
13. Combine the modified Y channel with the original Cb and Cr channels to form the watermarked YCbCr image.
14. Convert the watermarked YCbCr image back to the RGB color space using the 'ycbcr2rgb' function to obtain the final watermarked image 'y'.

The algorithm aims to embed the watermark in a perceptually invisible manner by modifying the DCT coefficients of selected blocks in the Y channel while considering the pseudorandom permutation to enhance security.

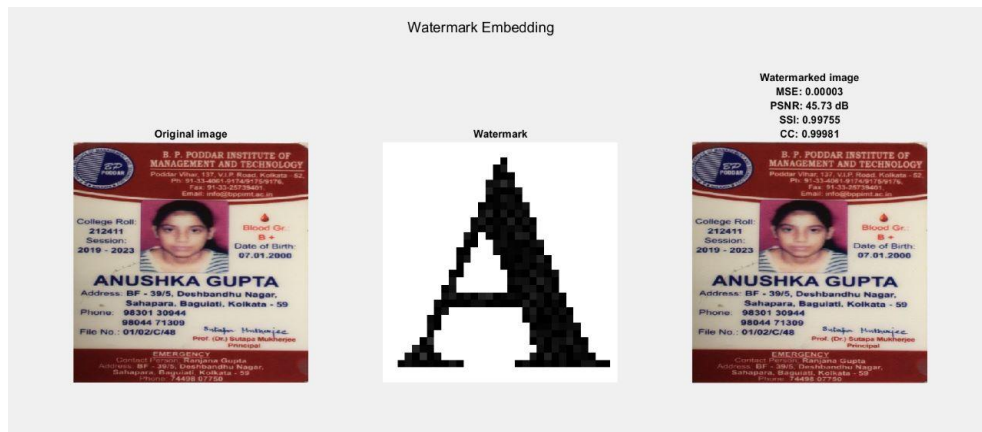


Fig 5 : Watermark Embedding

Extraction Algorithm:

The provided code implements the extraction stage of a blind watermarking algorithm that uses the Discrete Cosine Transform (DCT). The algorithm takes an original image 'x', a watermarked image 'y', and a key as input, and it returns the original image without the watermark ('x') and the extracted watermark.

Here is a step-by-step explanation of the algorithm:

1. Convert both the original image 'x' and the watermarked image 'y' from the RGB color space to the YCbCr color space using the 'rgb2ycbcr' function.
2. Extract the Y-channel from both the original and watermarked YCbCr images.
3. Divide both the original and watermarked Y-channels into 8x8 blocks and apply the DCT (Discrete Cosine Transform) to each block. The resulting DCT coefficients are stored in separate cell arrays 'x_blocks' and 'y_blocks'.
4. Calculate the number of blocks ('num_blocks') based on the size of the Y-channel.
5. Select a random set of blocks from the 'x_blocks' and 'y_blocks' arrays to extract the watermark. The selection is based on the key provided. The number of selected blocks is fixed at 1024.
6. Perform the extraction stage by comparing the DCT coefficient at position (4, 2) in each selected watermarked block with the corresponding coefficient in the original block. If the difference ('diff') is negative, assign the corresponding watermark bit as 0. If the difference is positive, assign the watermark bit as 1.
7. Reshape the extracted watermark bits into a 32x32 matrix to reconstruct the watermark image.
8. Return the original image without the watermark ('x') and the extracted watermark image.

The algorithm aims to extract the watermark by comparing the DCT coefficients of selected blocks in the watermarked image with the corresponding coefficients in the original image. The extracted watermark is then reconstructed as a binary image based on differences between the coefficients.

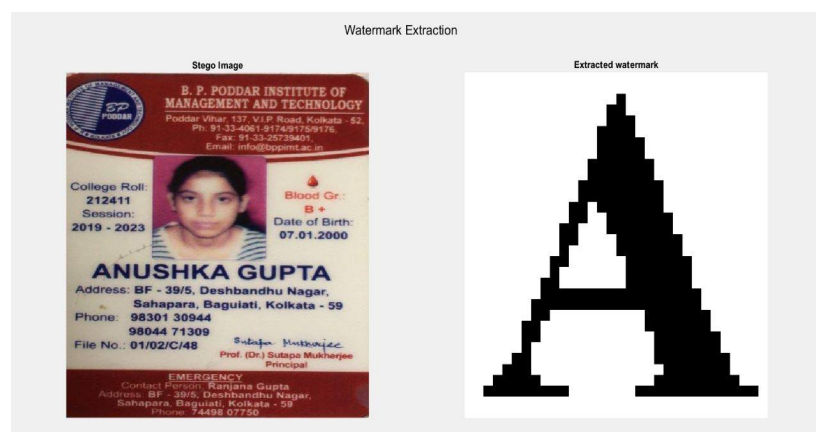


Fig 6(a) : Watermark Extraction without tampering

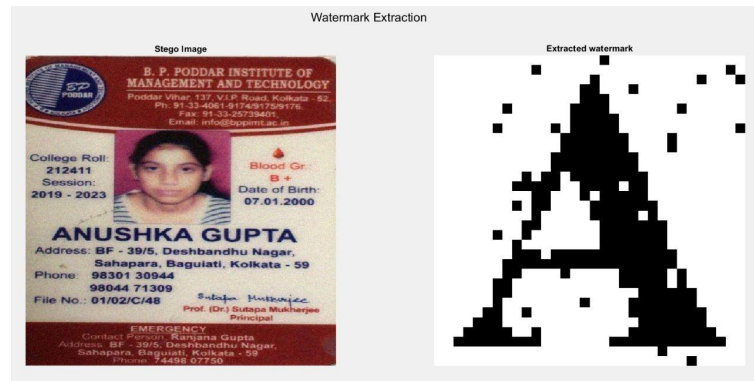


Fig 6(b): Watermark Extraction with tampering with 4% Gaussian Noise

Tampering Detection Algorithm:

- Step 1: At the Client Side: Input the Original cover image.
- Step 2: Hide the watermark image in the cover image using DCT and PN sequence.
- Step 3: Apply tampering on the Stego image and send it to the receiver.
- Step 4: During transmission, noise is incorporated (tampering will occur).
- Step 5: At the receiver, the image is tampered with noise is integrated and the receiver extracts the watermark image from the stego image.
- Step 6: For specific watermark image: Track the difference between similar color pixel byte elements within the concerned sub block image for both the original watermark and extracted watermark. Now, compute the ratio of two counter variables related to this difference based on a specific threshold value.

$$(a-c < 8, \text{ Cat1}++)$$

$$(b-d < 8; \text{ Cat2}++)$$
- Step 7: For specific watermark image: Compute the average value of all the sub-block elements for the concerned sub block Image for both the original watermark and extracted watermark image. Now, compute the ratio of two counter variables Related to this difference based on a specific threshold value.
- Step 8: For specific watermark image: Compute the similarity aspect of both the original and extracted watermark image in terms of standard parameters and based on specific threshold value the distortion aspect of the extracted watermark image can be judged.
- Step 9: Now, by evaluating the ratios found in Step 6, and Step 7 and the threshold value found in Step 8, the overall distortion scenario in the specific watermark image can be observed. Hence, by analyzing the quantified values tracked from Step 6, Step 7, and Step 8 the distortion cum tampering effect in the corresponding extracted watermark image can be decided.








Noise	Stego-Image	Tampered Stego-Image	Extracted Secret Image	Tampering Analysis
No Noise				16.99%
4% Gaussian Noise				19.82%
10% Salt & Pepper noise 45.12%				45.12%

Fig 7: Tampering Detection using different noises

Result Analysis:

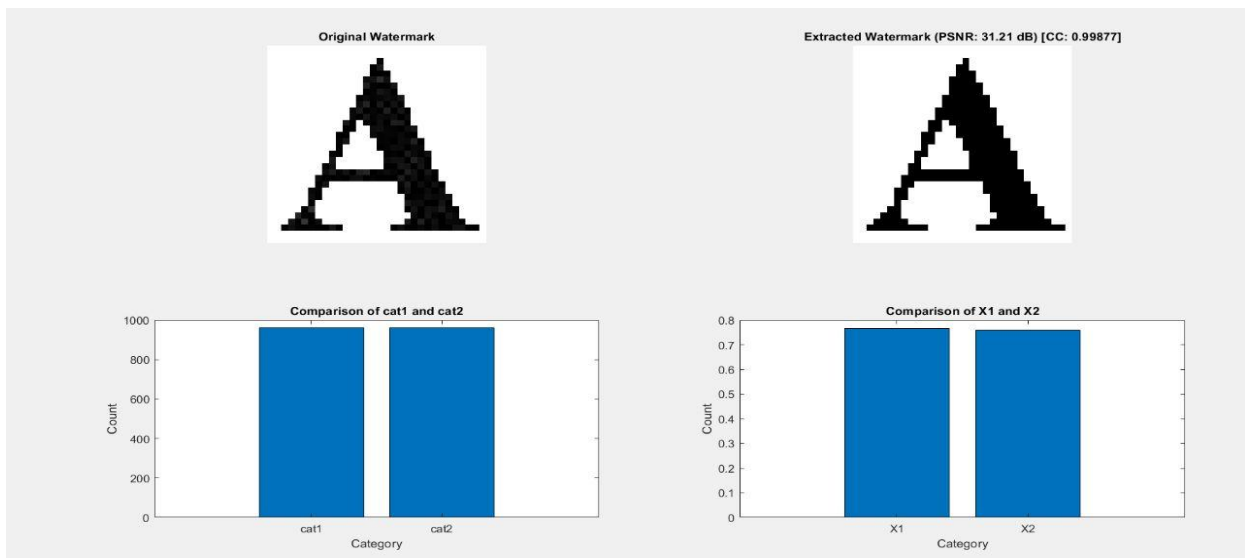


Fig 8.1 : Watermark without tampering

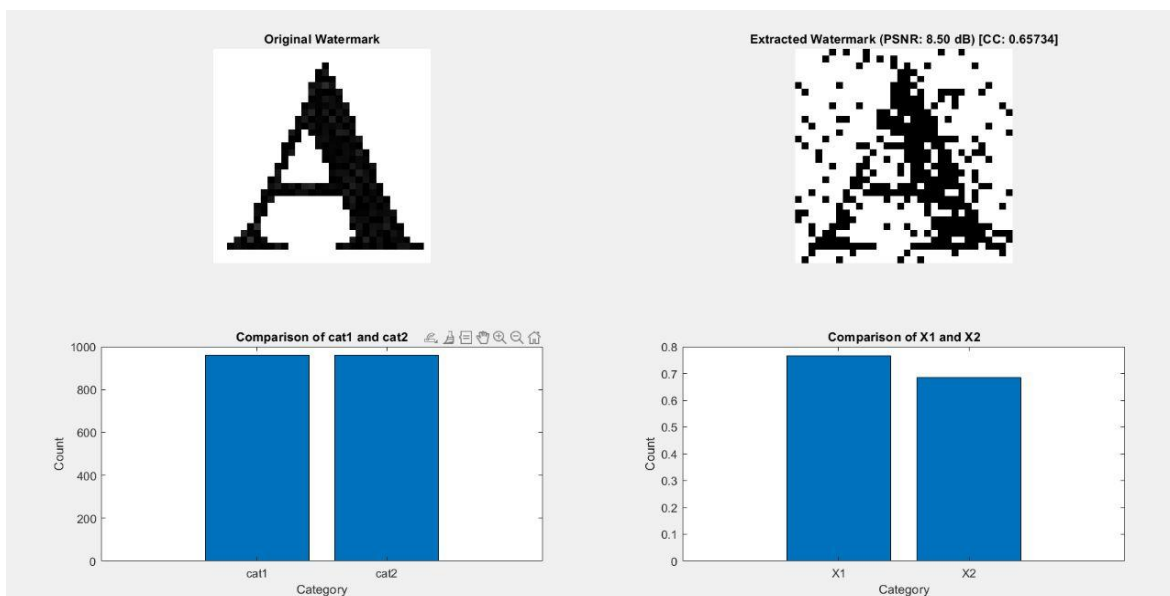


Fig 8.2 : Extracted Watermark from a tampered image

Fig (8.1) and (8.2) shows the histogram analysis of tampered watermark

Literature Review

Image authentication refers to the process of verifying the integrity and authenticity of digital images, ensuring that they have not been tampered with or modified without authorization. Steganography, as mentioned earlier, involves hiding information within an image while maintaining its visual appearance.

In paper [1] , have demonstrated that different data concealing strategies were considered. Data is encrypted using cryptography, and it is hidden behind a cover file using steganography. More security is offered by combining steganography with cryptography than by using either technology alone. The most popular kind of encryption that uses huge block sizes and encrypts data in blocks is AES. Video is the ideal option for a cover file in steganography process since it contains greater capacity compared to a picture or audio file, the data's ability to be embedded.

Tamper Detection techniques, according to Minati Mishra and Flt. Lt. Dr. M. C. Adhikary [2], is primarily based on Both activem and passive tamper detection methods have been the subject of much research, and there is still much work being done globally to effectively detect tampering in digital photographs. Splicing and cloning, two commonly employed passive detection approaches, have been discussed in this study. However, it's noteworthy to note that both tamper detection and tampering strategies are developing. The issue is becoming more difficult as newer iterations of detection resistant tampering methods are growing in response to the introduction of a new picture authentication and tamper detection approach.

Mahmoud Magdy , Neveen I. Ghali , Said Ghoniemy , Khalid M. Hosny , stated in a paper[3] In many eHealth applications, including storage, retrieval, identity theft, data management, and data security, image security is crucial. This paper includes a brief overview of certain well-known picture assaults that are used to assess the effectiveness of the suggested algorithms on images. To encourage more study in this field, we have outlined the cryptographic technique, its traits, varieties, needs, working environment for each approach, and potential challenges.

In order to build a more reliable, high authenticity, and high security watermarking, a number of studies and researches have been undertaken in paper[4]. In the area of digital image processing, a variety of watermarking techniques and algorithms are available.

In paper[5], This research examines the idea of steganography by first examining the definition of steganography and the terminologies connected to it. Using a technique called steganography, one may hide data inside of a picture by making a few minute changes.

In paper[6],[10] and [13], In this study, the use of the DWT, DCT, DFT, and LSB algorithms has been used to analyse watermarking in medical photographs. This study's objective is to compare the outcomes of several methods used to calculate PSNR and SR values on medical pictures. Using DCT, DWT, LSB, and DFT approaches, logo pictures are injected values on medical pictures. Using DCT, DWT, LSB, and DFT approaches, logo pictures are injected into medical imaging (MR) in this study, and several attacks are connected on the resulting images. The three MR pictures utilised are distinct. The DFT approach was determined to have the highest PSNR (48, 1430). DCT, DFT, and LSB values are essentially same. Their PSNR scores are in the 35 range. DFT SR values are the poorest when comparing the SR values of the DCT, DFT, and DWT approaches. embedding utilising frequency in MR images as a result.

In paper [7], Rajkumar Ramasamy and Vasuki Arumugam , In this article, they've covered a range of topics related to digital watermarking, such as its concepts, prerequisites, different domains with fundamental algorithms, and comparative metrics. They also made an effort to provide comprehensive fundamental information about digital watermarking, which will aid new researchers in gaining the most knowledge possible in this field.

Among the many important security objectives that cryptography aids in achieving are authentication, integrity, secrecy, and no-repudiation. Cryptographic algorithms are developed to achieve these goals. Providing trustworthy, solid, and dependable network and data security is the goal of cryptography. In this study of paper[14],it has been summarised some of the research on the topic of cryptography and described the operation of the many cryptographic algorithms used for different security objectives. Cryptography will continue to be employed in IT and business planning to safeguard personal,financial,medical, and e-commerce data while retaining a fair amount of privacy.

Deepika Sharma , Pawanesh Abrol discusses in paper [12] that the ability to transmit digital images using imaging technologies like digital cameras, scanners, photo-editing, and software packages has significantly increased over the past few years as a result of significant advancements in computing and network technologies as well as the availability of better bandwidths. The application of this technique, however, also extends to the manipulation of digital photos and the production of convincing photocopies. As a result of the easy availability of digital photos and the availability of free image altering tools, there is a growing challenge with determining the authenticity of digital photographs.

In paper[11], Pranali R. Ekatpure, Rutuja N Benkar, demonstrated that it is impossible to state with certainty that Steganography can be used as an alternative to cryptography after an unsatisfactory comparison. Although cryptography provides services that are more secure, there are certain drawbacks. This does not, however, establish categorically that Steganography cannot be used in place of cryptography. Steganography and cryptography are used in this way to address all security concerns.

Rayana, Vatsa Agarwal, Sumita Gupta ,stated in their article [9] that by evaluating the works that have made significant findings in the area of data protection employing encoder decoder designs, this research article conducted a comparison investigation. This study assesses the neural networks capacity to carry out the necessary task to a particular level of fineness, which can serve as the foundation for upgraded and more deeply trained models in the future. The outcomes of the two designs, one for single-image steganography and the other for multi-image steganography, were compared to our earlier implementations using imperceptibility as a success measure in the study.

Adrian Morales-Ortega and Manuel Cedillo-Hernandez demonstrated in their review paper [8], A zero-watermarking method for digital photographs is presented in this study. With this approach, we extend the capabilities of the zero-watermarking algorithm to identify tampering in digital pictures using only one watermark signal, unlike current systems that primarily focus on ownership authentication. Results from experiments demonstrate the reliability of ownership identification proof and the ability to spot manipulated information. In our upcoming study, we'll investigate a data-hiding method that makes it possible to securely disguise the zero watermarking code inside the image content and so enhance the administration of the zerowatermarking codes.

Ziyue Xiang and Daniel E Acuna,in their article[16] ,For scientific photos, they have put forth a brand-new image tampering detection technique that is focused on finding noise discrepancies. Also created residual pictures to take use of the image's noise pattern, and they created a novel feature extraction method to reduce the problem's dimensionality so that a lightweight classifier can handle it. A fresh scientific picture collection comprising western blots and microscope imaging is used to evaluate the approach. The findings show that their approach is able to detect different forms of picture

manipulations better and more consistently when compared to two base line methods that are widely used in the literature. Consequently, their approach promises to successfully address a significant aspect of picture manipulation in research.

Table 1: Comparison between the proposed method and methods by [Huynh-The et al. \(2016\)](#) and [Liu \(2012\)](#).

	Thien Huynh-The et al.	Liu K. C	Proposed method
Host image size	512 x 512	512 x 512	512 x 512
Image type	Color	Color	Color
watermark	32 x 32	32 x 32	32 x 32 (bitmap)
Technique used	4-Level DWT	LSB Replacement	DCT & PN Sequence
PSNR	43.51	39	47.78

Conclusion:

In conclusion, this paper presented a method for embedding a 32x32 bitmap image within a 512x512 cover image using Discrete Cosine Transform (DCT) and a Pseudo-Noise (PN) sequence. The embedding process involved converting the original image to the YCbCr color space, generating a PN sequence using a securitykey, and permuting the Y-channel of the cover image. DCT was applied to 8x8 blocks of the permuted frame, and a selected number of random blocks were used to embed the watermark pixels. The process was reversed to extract the embedded image from the cover image. Additionally, tampering detection was incorporated into the algorithm to ensure the integrity of the embedded image. The tampering detection process involved tracking differences between the original watermark and the extracted watermark, computing ratios of these differences, and comparing them to predefined threshold values. The average values of sub-block elements in both images were also compared using counter variables and threshold values. Finally, the distortion and tampering effect in the extracted watermark image were evaluated based on the calculated ratios and thresholds. The proposed method provides a secure and robust approach for embedding and extracting a secret image while detecting tampering and noise. By analyzing the quantified values obtained through the tampering detection process, the distortion and tampering effects in the extracted watermark image can be accurately determined. This technique holds promise for applications where data integrity and confidentiality are paramount, such as digital watermarking, copyright protection, and secure communication. Only two algorithms have been used to calculate the pixel variations. In future more effective algorithms can be used to attain more accuracy and precision. Such algorithms could more efficiently detect even the smallest of tampering. That means we may be able to detect the position of manual tampering more precisely and can pin point the location. Also we can use more complex algorithm for encoding and decoding to increase the security and confirm authenticity.

Future Scope:

The future scope of image tampering detection using noise is promising, as advancements in technology and image processing algorithms continue to evolve. As tampering detection algorithms improve, there may be a demand for integrating these algorithms directly into image editing software. This integration can help users identify potential tampering in real-time and promote responsible image manipulation practices. With privacy concerns becoming more prominent, future research may explore privacy-preserving techniques for tampering detection. This can involve developing algorithms that can analyze image noise without compromising sensitive information or violating user privacy. Overall, the future of image tampering detection using noise holds significant potential for advancements, ranging from algorithmic improvements to integration with various applications and addressing emerging challenges in the field.

Acknowledgement:

We would like to express our sincere gratitude to our mentor, Ms. Sudipta Roy, for her invaluable guidance and support throughout the development of the proposed embedding algorithm and Tampering detection and analysis for secure image steganography. Her expertise and insightful suggestions have been instrumental in shaping the direction and execution of this research. Ms. Sudipta Roy's profound knowledge in the field of steganography and cryptography has greatly influenced our understanding of the subject matter. Her guidance helped us navigate through complex concepts and methodologies, ensuring that our algorithm adhered to the highest standards of security and efficiency.

We would also like to acknowledge her role in fostering a collaborative and conducive research environment. His open-mindedness and willingness to listen to our ideas have facilitated meaningful discussions and critical thinking, contributing to the overall success of this project. We extend our deepest appreciation to Ms. Sudipta Roy for her unwavering support, mentorship, and guidance. Her expertise, patience, and encouragement have been indispensable to our research journey, and we are sincerely grateful for the opportunity to work under her supervision.

References

- [1] Aiswarya.S , Gomathi.R, “Review On Cryptography and Steganography Techniques in Video” in IEEE conference 2018
- [2] Minati Mishra , Flt. Lt. Dr. M. C. Adhikary , “Digital Image Tamper Detection Techniques - A Comprehensive Study” in International Journal of Computer Science and Business Informatics 2013
- [3] Mahmoud Magdy , Neveen I. Ghali , Said Ghoniemy , Khalid M. Hosny , “Image Cryptography: A Systematic Review” in DMT Department, Future University in Egypt (FCIT) Cairo, Egypt 2016
- [4] Arshad Jamal, Mohammed Hazim Alkawaz , Mariam-Aisha Fatima, Mohd Shukri Ab Yajid , “Digital Watermarking Techniques And its Application Digital Halal Certificate: A Survey” 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC 2019), 13–14 December 2019, Melaka, Malaysia
- [5] Abhinav Agarwal , Prof. Sandeep C 2019), 13–14 December 2019, Melaka, Malaysia Malik, “A Brief Review on Various Aspects of Steganography ,Followed by Cryptographic Analysis” 2022 IEEE 7th International conference for Convergence in Technology (I2CT)
- [6] Volkan Kaya, Ersin Elbasi, “Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms” in IEEE Conference 2022
- [7] Rajkumar Ramasamy and Vasuki Arumugam, ”Digital watermarking —A tutorial” in IEEE Conference 7 July 2022
- [8] Adrian Morales-Ortega and Manuel Cedillo-Hernandez , “Ownership Authentication and Tamper Detection in Digital Images via Zero-Watermarking” 2022 45th International Conference on Telecommunications and Signal Processing (TSP) | 978-1-6654-6948-7/22/\$31.00 ©2022 IEEE | DOI: 10.1109/TSP55681.2022.9851253
- [9] 1Rayana, 2Vatsa Agarwal, 3 Sumita Gupta , “Image Steganography using Encoder - Decoder Architectures” 1, 2, 3Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Noida , 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) | 978-1-6654-9602-5/22/\$31.00 ©2022 IEEE | DOI:10.1109/COM-IT-CON54601.2022.9850662
- [10] Mahbuba Begum ,* and Mohammad Shorif Uddin, “Digital Image Watermarking Techniques: A Review” Information 2020, 11, 110; doi:10.3390/info11020110
- [11] Pranali R. Ekatpure, Rutuja N Benkar, “A Comparative Study of Steganography & Cryptography” International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

- [12] Deepika Sharma , Pawanesh Abrol, “Digital Image Tampering – A Threat to Security Management” , International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013
- [13] A. Mohanarathinam, S. Kamalraj, G. K. D. Prasanna Venkatesan, Renjith V. Ravi, C. S. Manikandababu , “Digital watermarking techniques for image security: a review” Received: 9 April 2019 / Accepted: 12 September 2019 / Publishedonline: 20 September 2019 © Springer-Verlag GmbH Germany, part of Springer Nature 2019
- [14] Shreyas M , Sudarshan U B, Rahul Verneker , Mrs. Ankitha S , Mr. Sayeesh, “A Review Paper on Cryptography” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 2, Issue 2, March 2022.
- [15] Gurdeep Singh¹, Prateek Kumar², Nishant Taneja³, Gurpreet Kaur⁴ , “ A RESEARCH PAPER ON CRYPTOGRAPHY” International Journal For Technological Research In Engineering Volume 7, Issue 4, December-2019
- [16] Ziyue Xiang and Daniel E Acuna, “Scientific Image Tampering Detection Based On Noise Inconsistencies: Method And Datasets” <https://ori.hhs.gov/education/products/RIandImages/guidelines/list.html>
- [17] Jobin Abraham , Varghese Paul, “An imperceptible spatial domain color image watermarking scheme” Journal of King Saud University – Computer and Information Sciences 31 (2019) 125–133
- [18] Liu, K.C., 2012. Color image watermarking for tamperproofing and pattern based recovery. IET Image Proc. 6 (5), 445–454.
- [19] Huynh-The, Thien, Banos, Oresti, Lee, Sungyoung, Yoon, Yongik, Le-Tien, Thuong, 2016. Improving digital image watermarking by means of optimal channel selection. Expert Syst. Appl. 62, 177–189.