International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

IMPLEMENTATION OF A SECURED WATERMARKING MECHANISM BASED ON CRYPTOGRAPHY AND BIT PAIR MATCHING

Sanjeevini s harwalkar[1], M.M.Praisy[2], P.Anusha[3], S.Dhanandhuka[4]

[1] Assistant Professor, Department of IT,Malla Reddy Engineering College For Women (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

[234]UG Scholar, School of CS,Malla Reddy Engineering College for Women, (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100
Email : Sanjeevini706@gmail.com

ABSTRACT

Watermarking is a critical technique for digital information protection, often used alongside cryptographic methods to enhance the security of digital data. In image watermarking, the Least Significant Bit (LSB) substitution method is commonly used to embed the watermark within the cover image. This paper introduces a novel approach that combines bit pair matching with symmetric key cryptography for watermarking.In this approach, the pixel bits of the original image and the encrypted watermark image are grouped into pairs. According to the proposed algorithm, the pixel bit pairs are arranged and compared between the encrypted watermark and the original image. If a matching bit pair is found, the respective matched pair is replaced with the binary equivalent of the pair's assigned number. In cases where no match is found, the 0th bit pair is replaced with the watermark bits, and the two least significant bits (LSB) are adjusted to reflect the pair number 0.The proposed technique demonstrates excellent quality in the watermarked image and achieves high Peak Signal-to-Noise Ratio (PSNR) values, indicating good image quality preservation. Furthermore, it provides a strong payload for the watermark. When compared with existing watermarking methods, the proposed scheme shows significantly improved performance, making it a valuable contribution to the field of image watermarking.

Keywords- Watermarking, Digital Information Hiding,Cryptography, Least Significant Bit (LSB) Substitution

I. INTRODUCTION

Digital watermarking is a technique widely employed for copyright protection in the digital age, aimed at safeguarding multimedia content from unauthorized reproduction and distribution. This technique involves embedding hidden or invisible information into a carrier medium—such as images, videos, audio, or even text—to establish ownership or verify the authenticity of the content. The main objective of watermarking is to provide a means of securing digital assets against piracy or theft while maintaining the quality and integrity of the original content.Watermarking is primarily used in the context of visible media, like images and videos, but its applications extend to other forms of digital media, such as audio files, documents, and software. The embedded

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

watermark, which could be text, a logo, or other identifying information, is imperceptible to the human eye or ear, ensuring that it doesn't interfere with the user experience. However, it can be detected through specific algorithms or techniques, enabling the owner to prove their claim over the content in case of infringement. While watermarking is designed to secure intellectual property by embedding identifying information into the media itself, it differs from fingerprinting. Both are related to steganography, but they have distinct purposes. Watermarking focuses on protecting the entire piece of content, often signifying ownership, copyright, or authorship. The "watermark" acts as a signature or identifier, which is consistent across all copies of the media, serving as a form of copyright protection.Fingerprinting, in contrast, embeds unique identifiers into different copies of the same content. These identifiers are designed to trace and identify individual copies, providing a way to track how the content is distributed. Unlike watermarking, which targets content ownership, fingerprinting is primarily used to track the usage and distribution of specific copies, making it particularly useful in cases where unauthorized sharing or piracy is suspected. Fingerprints are often tailored to individual users or specific copies, allowing the owner to identify the origin of leaks or unauthorized copies.

Both watermarking and fingerprinting are essential tools in the digital rights management (DRM) ecosystem, with watermarking protecting the overall content and fingerprinting ensuring traceability and accountability for distributed copies. Together, they form a robust defense against content piracy and unauthorized use in the digital world.

II. RELATED WORK

1.Least Significant Bit (LSB) Watermarking

One of the simplest and oldest methods for digital watermarking is Least Significant Bit (LSB) watermarking, where the watermark is embedded in the least significant bits of the pixel values of an image. This method is easy to implement and computationally inexpensive. However, it has several limitations. The primary drawback is its low robustness against attacks such as compression and noise. LSB watermarking can easily be detected and removed if the image undergoes transformations like resizing or compression, which makes it less suitable for applications requiring high security.

2. Frequency Domain Watermarking

To improve upon LSB watermarking's limitations, frequency domain watermarking methods were introduced. These techniques embed the watermark in the frequency domain, typically using methods like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Frequency domain watermarking provides better robustness against attacks such as compression, cropping, and filtering, as it is more resistant to changes in the image's spatial domain. However, the major drawback of frequency domain methods is that they require more computational resources, and excessive embedding may lead

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

to degradation in the visual quality of the image.

3. Spread Spectrum Watermarking (SSW)

Another significant method is Spread Spectrum Watermarking (SSW), where the watermark is spread over a wide frequency spectrum. This technique improves the robustness of the watermark against a variety of attacks such as noise, cropping, and compression. However, the trade-off is reduced imperceptibility because the watermark signal is spread across the spectrum, which can result in noticeable distortions in the watermarked content. Despite these drawbacks, SSW offers a good solution for applications where watermark robustness is more critical than imperceptibility.

4. Hybrid Watermarking Techniques

Hybrid watermarking techniques combine the strengths of both spatial and frequency domain methods. These approaches aim to provide a balance between robustness, imperceptibility, and embedding capacity. By incorporating features from both domains, hybrid methods try to address the weaknesses of each individual technique, such as the imperceptibility of frequency domain methods and the low robustness of spatial domain methods. However, these hybrid techniques tend to be more complex to implement and require higher computational power, making them less feasible for real-time or resource-constrained applications.

5. Cryptography-Based Watermarking

In recent years, cryptography-based watermarking techniques have gained popularity as a means of enhancing security. These methods use encryption algorithms to secure the watermark, ensuring that only authorized parties can extract and verify it. Cryptography-based watermarking ensures the authenticity of the content and prevents unauthorized modification or removal of the watermark. While these techniques provide high security, they often require more computational resources and may have an impact on the overall efficiency and performance of the watermarking system.

Each of these techniques has its advantages and drawbacks, and their application depends on the specific requirements of the multimedia content and the level of security, robustness, and imperceptibility required for a given application.

III. IMPLEMENTATION

1. Image and Watermark Selection

The proposed digital watermarking scheme starts by loading the original cover image, which can be either a grayscale or color image. If it's a color image, it may be converted to grayscale for simpler processing. Next, the watermark is selected, which could be a text or image.

2. Encryption of Watermark

The watermark is then encrypted using a symmetric key encryption algorithm like AES or DES to secure it. The encrypted watermark is then prepared by converting its pixel values into binary form.

3. Bit Pair Matching

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

The core of the watermarking process is the **bit pair matching**. In this step, both the original image and the encrypted watermark are represented as pairs of bits. These bit pairs from the encrypted watermark are compared with the bit pairs from the cover image. If a matching pair is found, the corresponding bit pair from the original image is replaced with the watermark bit pair. If no match is found, the algorithm replaces a specific placeholder bit pair with the watermark bit.

4. Embedding Watermark in LSB

The watermark is embedded in the **least significant bits (LSBs)** of the image pixels to maintain the quality of the image. This method ensures that the watermark is embedded securely without significantly affecting the image quality.

5. Generation of Watermarked Image

Finally, the resulting **watermarked image** is generated, and its quality is evaluated using parameters like **Peak Signal-to-Noise Ratio (PSNR)** and **payload capacity**. The proposed method is compared with existing watermarking algorithms to demonstrate its effectiveness in terms of image quality and security.

IV. ALGORITHM USED

1.Cryptographic Algorithms :

Cryptographic algorithms are crucial for securing the watermarking process and ensuring that the watermark is resistant to attacks and unauthorized modifications. These include:

Hashing Algorithms (SHA-256)

Hashing algorithms like **SHA-256** are used to generate a unique fingerprint or hash of the watermark data. This ensures that any modification to the watermark can be detected by comparing the generated hash during extraction.

$$H(m) = \text{SHA-256}(m)$$

Where:

- H(m) is the hash of the message (watermark data).
- m is the watermark data.

Symmetric Encryption (AES)

The **Advanced Encryption Standard (AES)** algorithm is used to encrypt the watermark data before embedding it in the host media. AES ensures that even if an attacker gains access to the watermark, they cannot easily extract or tamper with it.

$$C = \text{AES}(P, K)$$

Where:

- C is the ciphertext (encrypted watermark).
- P is the plaintext watermark data.
- K is the encryption key.

Asymmetric Encryption (RSA)

For additional security, asymmetric encryption techniques like **RSA** can be used to securely transmit the encryption key or watermark data in public environments.

$$C = P^e \mod n$$

Where:

- C is the ciphertext.
- P is the plaintext (watermark data or key).
- e is the public exponent.
- n is the modulus (product of two primes).
- The decryption is performed using the private key.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

2,Watermark Embedding Using Bit Pair Matching (BPM)

The **Bit Pair Matching (BPM)** algorithm is used for embedding a watermark in the least significant bits (LSB) of the host image pixels. This algorithm is effective because it allows for a high degree of imperceptibility of the watermark.

Process of BPM Algorithm:

The BPM algorithm works by matching pairs of bits from the watermark with the least significant bits of the pixels in the image.

Extract pairs of bits from the watermark (for example, for a binary watermark).

Let's assume we have a watermark represented as a binary sequence:

$$W = w_1, w_2, w_3, ..., w_n$$

Identify pixel values in the image (in terms of their bit pairs). Let's say a pixel P(x,y)P(x, y)P(x,y) has the following 8-bit representation:

$$P(x, y) = p_7, p_6, p_5, p_4, p_3, p_2, p_1, p_0$$

Formula for embedding:

$$P'(x, y) = P(x, y) \oplus (p_1, p_0) \oplus (w_{2i}, w_{2i+1})$$

Example:

For a 4-bit pixel:

- Original pixel: $P(x, y) = 11010101$
- Watermark bits: $w = 01$
- Embedding:

$$P'(x, y) = 11010101 \oplus (01) = 1$$

V. RESULTS

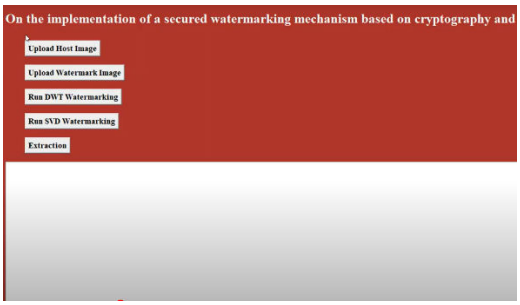

Fig 1: Upload Host Image

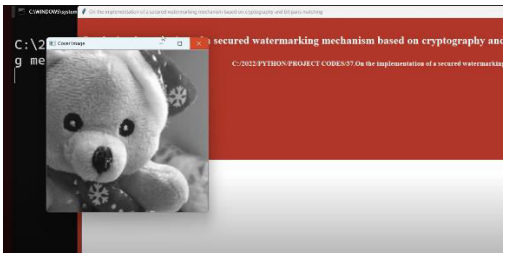

Fig 2 : Upload Watermark Image

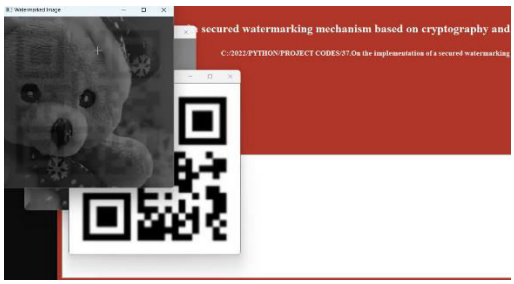

Fig 3 :Run Dwt Watermarking

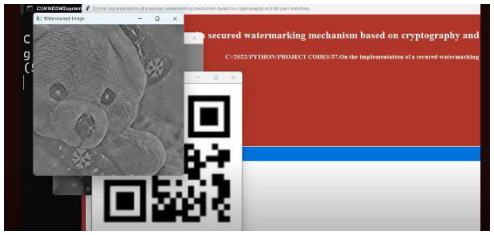

Fig 4 : Run SVD Watermarking

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

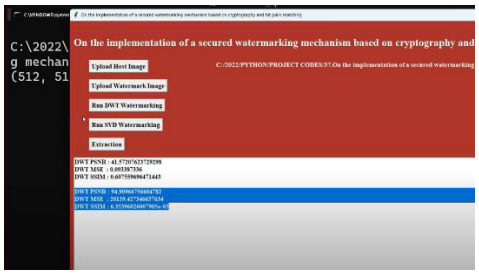

Fig 5 : Extraction

VI. CONCLUSION

In this paper, a novel watermarking technique is introduced, which utilizes bit-pair similarity for Least Significant Bit (LSB) replacement. Unlike traditional watermarking methods, which focus on modifying individual bits in the image, this technique leverages the similarity between bit pairs, providing a unique approach to embedding a watermark. This method is distinct from existing techniques, as it introduces a new paradigm for bit manipulation, focusing specifically on the relationship between pairs of bits rather than isolated individual bits.To ensure the security of the watermark, the proposed method integrates symmetric key cryptography. By using this cryptographic technique, the watermark can be encrypted and securely embedded within the host image. Symmetric key cryptography is crucial because it allows both the sender and the receiver to use the same key for both encryption and decryption, ensuring that only authorized parties can access or retrieve the watermark information.The technique works by arranging the data bits in pairs, which is a departure from conventional approaches where bits are typically manipulated one at a time. This pairing of bits creates a more complex structure, making the watermarking process more secure against unauthorized extraction or tampering. By embedding the watermark in this paired format, the method enhances both security and robustness, making it more difficult for attackers to successfully alter or remove the watermark without causing noticeable damage to the image.The proposed method was tested on 15 different grayscale images, and the experimental results demonstrated several key advantages over traditional methods. The technique offers higher security due to the use of cryptographic protection and bit-pair similarity, which significantly improves the robustness of the watermark against common attacks such as cropping, resizing, or compression. Additionally, the method supports a higher payload, meaning it can embed more data within the image without sacrificing quality or imperceptibility.

Imperceptibility refers to the ability of the watermark to remain hidden or undetectable to the human eye, and this technique achieves excellent results in this regard. The watermark remains invisible under normal viewing conditions, ensuring that the host image's visual quality is preserved. The experiments showed that the proposed method strikes an optimal balance between high payload capacity, security, robustness, and imperceptibility, making it a significant advancement in the field of digital watermarking.

REFERENCES

[1] Khan, F., Gutub, A.A.A., 2007. Message concealment techniques using image based steganography.

[2] Gutub, A., Al-Qahtani, A., Tabakh, A., 2009. Triple-A: secure RGB image steganography based on randomization.

[3] Al-Otaibi, N.A., Gutub, A.A.A., 2014. Flexible stego-system for hiding text in images of personal computers based on user security priority.

[4] Altaibi, N.A., Gutub, A.A., Khan, E.A., 2015. Stego-system for hiding text in images of personal computers.

[5] Gutab, A.A.A., Ghouti, L., 2007. Utilizing extension character 'Kashida' with pointed letters for arabic text digital watermarking. 5. Hannigan, B.T., Reed, A., Bradley, B., 2001. Digital watermarking using improved human visual system model.

[6] Roy, B., Rakshit, G., Singha, P., Majumder, A., Datta, D., 2011. An improved symmetric key cryptography with DNA based strong cipher.

[7] Vleeschouwer, C.D., Delaigle, J., Macq, B., 2001. Circular interpretation of histogram for reversible watermarking.

[8] Wang, C., Li, X., Yang, B., Liu, Lu.C., 2010. A content-adaptive approach for reducing embedding impact in steganography.

[9] Hempstalk, K., 2006. Hiding behind corners: using edges in images for better steganography.

[10]Sabeti, V., Samavi, S., Shirani, S., 2013. An adaptive LSB matching steganographybased on octonary complexity measure. Multimedia Tools

[11]Sharp, T., 2001. An implementation of key-based digital signal steganography.

[12]Sumathi, C., Santanam, T., Umamaheswari, G., 2014. A study of variousssteganographic techniques used for information hiding.

[13]Swanson, M.D., Kobayashi, M., Tewfik, A.H., 1998. Multimedia data embedding andwatermarking technologies.

[14]Tsai, Y., Huang, Y., Lin, R., Chan, C., 2016. An Adjustable interpolation based datahiding algorithm based on LSB substitution and histogram shifting.

[15] Wang, C.M., Wu, N.I., Tsai, C.S., Hwang, M.S., 2008. A high quality steganographicmethod with pixel-value differencing and modulus function.

[16] Wu, D.C., Tsai, W.H., 2003. A steganographic method for images by pixel-valuedifferencing.

[17] Xia, Z., Wang, X., Sun, X., Liu, Q., Xiong, N., 2016. Steganalysis of LSB matching usingdifferences between nonadjacent pixels.

[18] Xuan, G., Zhu, J., Chen, J., Shi, Y.Q., Ni, Z., Su, W., 2002. Distortionless data hidingbased on integer wavelet transform.

[19] Yang, C.H., Weng, C.Y., Wang, S.J., Sun, H.M., 2008. Adaptive data hiding in edgeareas of images with spatial LSB domain systems.

[20] Hu, Y., Lee, H.K., Li, J., 2009. DE-based reversible data hiding with improvedoverflow location map.

[21] Haung F., Zhong, Y., Huang, J., 2014. Improved algorithm of edge adaptive imagesteganography based on LSB matching revisited algorithm.