SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Enhancing Image Security: A Hybrid Asymmetric Cryptosystem For Robust Watermarking With Comparative Performance Analysis

Yandapalli Venkata Sree Vaishnava Reddy[1] , Davanam Ganesh[2]

[1]Research Scholar, Department of CSE, Mohan Babu University, Tirupati, Andhra Pradesh, India. yvreddy008@gmail.com
[2]Associate Professor, Department of CSE, Mohan Babu University Tirupati, Andhra Pradesh, India. dgani05@gmail.com

Abstract:
There is a storm of digital data being kept and published on public platforms like LinkedIn, Facebook, Twitter, and others due to the explosion of AI-powered smart devices and the Internet of Things (IoT). Of them, digital pictures are by far the most popular means of disseminating information. According to recent statistics, Google Photos stores more than one billion photographs per week. Furthermore, digital images are vital in many fields and applications, such as business, legal systems, social media, smart healthcare, autonomous vehicles, robotics, the film industry, and industrial automation. But there are serious privacy and security issues with these pictures being misused. An increasingly serious problem in the modern day, identity theft is one of the main causes of fraud in India and other nations. Therefore, protecting digital photos is an important problem that must be solved. The best way to protect digital photographs without breaking the bank is to use watermarking techniques. To make digital content more resistant to modification and ensure its longevity, digital image watermarking has become an indispensable tool. Nevertheless, because to the fact that each method is typically only applicable to certain applications, no digital watermarking solution now available provides total security against all types of attacks. A recent development in information security has been the incorporation of deep learning methods, which have been beneficial to this area. To protect the watermarked photographs from intruders, we will present a new and strong Hybrid Asymmetric Image Cryptosystem (HAIC) method in this paper. In addition, we have proved that our suggested system outperforms the current systems by comparing our work to similar systems that already exist.

Keywords- Watermarking digital images, steganography, and AI Data masking, protection.

1. Introduction:

Data transmission has become more efficient and less laborious due to the development of computer networks and telecommunications. Having so many options for programs and tools has made us more susceptible to cybercriminals [1]. Developing an effective technique to secure digital images and other multimedia data with copyright is becoming more and more of a challenge. Cryptography, steganography, & digital watermarking are only a few of the security measures that are necessary to safeguard multimedia data [2]. Encryption and decryption are two parts of cryptography that work together to protect data in both text and graphic formats. Data remains vulnerable once decrypted, although this does allow for secure communication between parties. Typically, cryptographic techniques alter signals such that they are understandable by anybody who intercepts them. Steganography allows trusted parties to communicate covertly while carrying a modest payload.

To guarantee secret communication, it is a method that inserts hidden data into cover images [3]. In most cases, a key is needed to embed the data; without this key, it would be very impossible for an unauthorized individual to uncover or extract the concealed information. The steganographic image is the one that contains the hidden data. Because of its primary purpose—the protection of sensitive information—steganography must be robust against attacks, data revisions, and possible alterations while transmission, storage, or format conversion. There is no competition between steganography and

watermarking; rather, the two technologies work hand in hand. Several uses for watermarking are seen in figure 1..

Figure 1. various watermarking applications

Because they may keep the original image quality while adding extra information, image methods for watermarking have become quite popular in many fields. Because of the critical nature of medical & military imaging, this is of the utmost importance. Integrating diagnostic records, medical pictures, and other pertinent information into medical cover photos has grown crucial with the healthcare sector's shift to Electronic Health Records (EHR) [4]. The use of watermarks in medical images has several advantages, including better data security, more reliable images, and more privacy for patients and doctors alike [5]. For the security and integrity of data in these sensitive businesses, reversible watermarking—which recovers the original image after watermark extraction—is critical. While there are reversible water-marking techniques available, they aren't always resilient enough to withstand deliberate and accidental assaults like noise addition and image compression. We devised a strong and reversible watermarking method to differentiate between assaults to solve these problems.

The ability to remove a watermark from a picture and return it to its original state is known as reversible watermarking. Spatial, frequency, or compression domain restoration is possible. The security of spatial domain techniques is lower compared to the other two. Histogram methods, LSB substitution, Differential Expansion (DE) [6], particle swarm optimization [7], evolutionary algorithms (GA), and the Firefly algorithm are some of the methods used to perform reversible water-marking. For reversible watermarking in the frequency domain, methods such as integer wavelet transform and integer DCT-based transform are employed.

However, the watermark isn't strong enough for practical applications, and the majority of the proposed lossless watermarking methods are inadequate. It is possible to compromise a watermark's recoverability by deliberate or passive attacks, noise introduction, or JPEG compression, among other unintended attacks [8]. One common technique for reducing the amount of space required to save photos is lossy compression. Medical images are compressed in telemedicine settings to reduce bandwidth requirements for effective image transmission. Consequently, picture compression is thought of as an accidental assault. As a result, we need reversible watermarking technology that can tell the difference between accidental and malicious attacks. Although they are resistant to accidental attacks, semi-fragile (or robust) water marks can be erased by intentional manipulation. The original medical image will be faithfully recreated after removing the watermark thanks to Particle Swarm Optimization (PSO) & wavelet transform, which ensure a high embedding capacity and robustness. Improving the embedding capacity of a reversible watermarking technique was achieved by employing an algorithm that merges the Integer with Discrete Gould Transform (DGT) [10] & Wavelet Transform (IWT) [11].

The privacy and security concerns around medical photographs prompted the development of a two-stage watermarking system, which involves inserting the watermark plus side information into two separate locations [12]. This technique avoids data over-lap by incorporating it into separate blocks using a Slantlet transform matrix. The watermarking algorithm utilizes the SVD approach, which stands for wavelet transform [13]. Data can be hidden and then retrieved via recursive dither modulation. The implanted watermark bits are vulnerable to geometric deformations, which is a common drawback among all these approaches.

Lorenz chaotic function adaptive waveform embedding in QR codes is one example of an optimized method in this developing area that improves security and prevents illegal data extraction [14]. Aerial remote sensing photos can now be securely protected using methods that combine singular value decomposition with redundant discrete wavelet transform [15].

Digital watermarking has recently seen significant improvements in security and robustness, which is particularly useful for applications that demand high levels of imperceptibility and attack resilience. Protecting sensitive photos while maintaining a balance between resilience and imperceptibility has been successfully achieved in the medical area using an improved watermarking strategy that is based on Arithmetic Wavelet Transforms and Particle Swarm Optimization [16]. An innovative method has been suggested that uses the Lorenz chaotic model to include chaotic encryption into digital images, making watermark embedding more secure and flexible [17]. A hybrid approach that incorporates both watermarking and optimization algorithms inspired by nature, like Particle Swarm Optimization and Firefly, yields the best scaling factor for secure embedding in E-health apps [18]. Watermarking has also made use of machine learning to boost efficiency; new research shows that it helps optimize choosing features for secure, durable watermarking on many types of media [19]. Meanwhile, cutting-edge watermarking techniques that combine the Curvelet transform with several chaotic maps have shown improved localization and imperceptibility, effectively tackling copyright protection & tamper detection [20]. These developments highlight a significant trend in watermarking, which aims to safeguard data integrity in embedded contexts by balancing imperceptibility, resilience, and security. This will strengthen the management of digital rights and improve information security in different applications. The invisibility, reversibility, and resilience of reversible watermarking are its defining characteristics. How perceptible the aberration is in the post-insertion watermarked image is what imperceptibility is measuring. A smaller amount of distortion is indicated by a higher imperceptibility value. When evaluating the security of watermarked photos, robustness is an important consideration. The ability to remove the watermark and return the cover to its previous state should be a top priority. Using a Slantlet transform matrix, this approach divides the data into non-overlapping chunks.

What follows is an outline of the remaining paper. The literature review of different watermarking security approaches is presented in Section 2. The proposed approach and the algorithms for encrypting and decrypting photos are detailed in Section 3. Section 4 discusses the experiments and the results, , whereas Section 5 concludes the work.

2. Literature Survey:

This section provides a synopsis of relevant previous study on digital video watermarking. Two well-known security tools, cryptography and digital signatures, are examined initially in this paper. Next, we'll go over the basics of digital watermarking, including its principles and methods. On top of that, the benefits and key distinctions between watermarking techniques and these other technologies are detailed.

The initial method of watermarking utilizing deep learning was developed by Kandi et al. [21]. Using several code books to generate images of varying sizes for embedding & extraction procedures, the authors introduced a CNN-based watermarking system. A lower image resolution is achieved by processing the host and inverted images using the algorithm. The relevant code books are rebuilt by upsampling the resultant image to a primitive level of precision. Using the acquired code book, the pixel values are changed to embed the BW. Guo et al. proposed a set of group normalization methods that would reduce resource usage during watermarking in their study [22]. They proposed employing CNN with a residual model. An approach to watermarking proposed by Hsu et al. [23] makes use of a fusion domain involving a super-resolution convolutional neural network (SRCNN) with the PSO algorithm. Before decomposing the host image, the QR technique couples its pixels. Hidden in the updated QR coefficients was the coded message. Adaptive convolutional neural network (CNN) blind watermarking was presented by Lee et al. [24]. To create the watermarked image, a network merges the watermark information with the cover image's modified channels. A CNN-based approach was introduced by Min Mun et al. [25]. Auto encoder (AE) and back propagation were two embedding strategies presented by the authors. Hidden in the little cover image's resolution were the coded secret bits. It was the decoder that received the encoded bits. The decoder creates a watermarked image that is sized to match the original image's resolution by using different strength factors.

An auto generator CNN-based watermarking system was introduced by Mahapatra et al. [26]. The feature maps of the host and watermark images are extracted and combined by the embedding network. In order to recover watermark data from the features that have been extracted, the RLU method is integrated into the block-level convolution extraction network. A fusion domain-based approach for medical pictures was introduced by Fan et al. [27] using the CNN- Inception V3 model and DCT. To

retrieve DCT-transmitted features, the initial Inception V3 network combined the host image. The encrypted watermark is encoded by the low-frequency magnitudes of the transformed medical picture characteristics. Using the MobileNetV2 model, DWT, and DCT, a composite algorithm for medical pictures was proposed by Nawaz et al. [28]. Using a hybrid chaotic system, the watermark vector of features was created. A hybrid domain watermarking technique was proposed by Li et al. [29] utilizing DCT and DarkNet53. DCT improves safety by extracting and fusing input medical picture features. To make medical images resistant to several geometrical attacks, Zhang et al. [30] suggested a composite watermarking method that uses GoogLeNet and Henon Map. In order to hide a random encrypted sequence in the host image, they combined several watermarked photos into one fully connected layer and encrypted it using the Henon map.

The methods of hybrid domain, which are based on transform domain, were suggested to increase the watermarking algorithm's resilience and resistance to conventional and geometric attacks. As of late, watermarking algorithms that use hybrid domains have taken center stage. The overall resilience and assault resistance of the watermarking algorithms could be enhanced with hybrid transform domain technology. Additionally, they raised the computational complexity simultaneously. A zero watermarking strategy against rotation attacks was proposed by Rui Wang [31] based on NSPD-DCT, and it demonstrated significant resilience to a variety of attacks. An encrypted watermarking approach utilizing Henon Map and the DTCWT-DCT domain was suggested by Jing Liu [32]. When considering encryption watermarks, the technique improves its anti-attack capabilities and can embed many watermarks simultaneously. By using the Arnold transform to encrypt the watermark data, Siming Xing [33] suggested an approach to make the data more secure. Attacks on image processing, such as clipping and rotation, were not able to weaken the method. Zermi Narima used DWT on retinal pictures and SVD on LL subbands in his proposal of the DWT-SVD method [34]. Although it fared poorly in scaling and rotating attacks, it was very resilient against noise attacks.

In order to incorporate an encrypted watermark, Balasamy K. [35] suggested a technique that makes use of fuzzy area of interest (ROI) and DWT. Despite its excellent security and resistance to conventional assaults, this algorithm was not as resilient to geometric attacks. In contrast, the watermarking methods proposed by Kahlessenane Fares [36]—"DCT-Schur" and "DWT-Schur"—were more resistant to JPGE compression attacks, with "DCT-Schur" standing out. The anti-attack capability of "DWT-Schur" was superior to that of 0.01 Gaussian noise. When it came to assaults that targeted scaling and average filtering, these two strategies failed miserably. A robust zero-watermark approach was presented by Feng ming Qin [37] using RSA pseudo-random sequence and Curve-let-DCT. This algorithm outperformed its counterparts in conventional and geometric attacks. The visual vectors of features of medical images were extracted using Bandelet-DCT. A new zero-watermarking approach for medical images was proposed by Yangxiu Fang [38]. It was highly resilient and used Scale Invariant Feature Transform (SIFT) during the preprocessing phase on the original medical image feature extraction. Cheng Zeng [39] presented a KAZE-DCT-based zero-watermarking medical image with good resilience.

When it came to protecting medical photographs against lossless copyright infringement, Zhiqiu Xia [40] suggested a zero-watermarking algorithm. This method was very resistant to both geometric and common attacks. In order to make the zero-watermark technique more secure, Baowei Wang [41] shown that it is possible to combine it with blockchain technology. A secure method for transforming multimedia was suggested by Ch. Rupa [42] using a chaotic logistic map that is based on deep learning. It was able to withstand a variety of cyberattacks because to its high entropy levels and ResNet model classification for detecting fraudulent medical multimedia data.

A long-lasting, undetectable, and secure method of photo watermarking was developed by Abdallah et al. [43] using Nonnegative Matric Factorization (NMF) and Fast Walsh- Hadamard Transformation (FWHT). The process consists of four stages: Before the watermark picture's singular values are evenly distributed among the modified blocks, the host image is first separated into small blocks and NMF is applied independently to each. Then, the weight matrix is generated using FWHT. A method for receiving-end picture authentication using information variables and digital signatures was suggested by Alam et al. [44]. Hyperchaotic (HCM) maps, 2-level SVD (Singular Value Decomposition), DCT, and DWT features were successfully utilized to increase the watermarking technique's security.

A new Cellular Automata (CA) using a DCT-based image watermarking system was presented by Jana et al. [45]. Zigzag scanning is performed after dividing a color cover image into red, green, and blue channels. Then, DCT is applied to 8 × 8 separate blocks of each channel in this system. For added protection, encrypt your digital images using CA rule-15 before adding a watermark. By merging Walsh Hadamard's Transform (WHT) with SVD, Helal et al. [46] created a digital picture watermarking system that meets the imperceptibility and robustness criteria while still being transparent. Using a combination

of Slant, Solitary Value Decomposition (SVD), and Quaternion Fourier-Transform (QFT), Eltoukhy et al. [47] presented a new, robust hybrid watermarking strategy for protecting color medical photos.

3.Methodology:

The HAIC, or Hybrid Asymmetric Image Cryptosystem, combines the mixing, diffusion, and confusion methods. The suggested method of encryption and unscrambling is shown in this section. The square chart of the proposed HAIC cryptography calculation is shown in Figure 3.1. The technique makes use of a secret key whose size can be adjusted. The blending procedure involves debasing a component of the original image. The incomplete encoded image that emerges is then divided into several non-covering key ward squared sectors. The diffusion and substitution tactics are used to prepare each square. Diffusion uses a multi-level saw-tooth SFC method to reorder the pixels inside each square. Confusion occurs when the surrounding pixels alter the attributes of each individual pixel. More precisely, neighboring pixels are dispersed broadly inside the image during the dissemination procedure. We carefully guard the execution of our dispersion and disarray operations. The totally jumbled image is the last product of the chaos stage. You can see the encryption algorithm in figure 2.The following section gives the detailed description about the encryption algorithm.

3.1 Plain Image

As a plain image, the encryption process utilizes the digital grayscale image. The size of the plain square photo can be changed with the mystery key.

3.2. Diffusion Process

This process involves swapping out one pixel for another in the image. A new pixel is generated by using open key to combine the characteristics of an existing pixel with those of an earlier pixel. This blending is accomplished by the EX-OR procedure.

$T_{x,y} = (T_{x,y} \oplus T_{x,y-1} \oplus E_i)(3.1)$

where E_i is the public key, $T_{x,y}$ is the current pixel element of original image and $T_{x,y-1}$ previous element value of image.

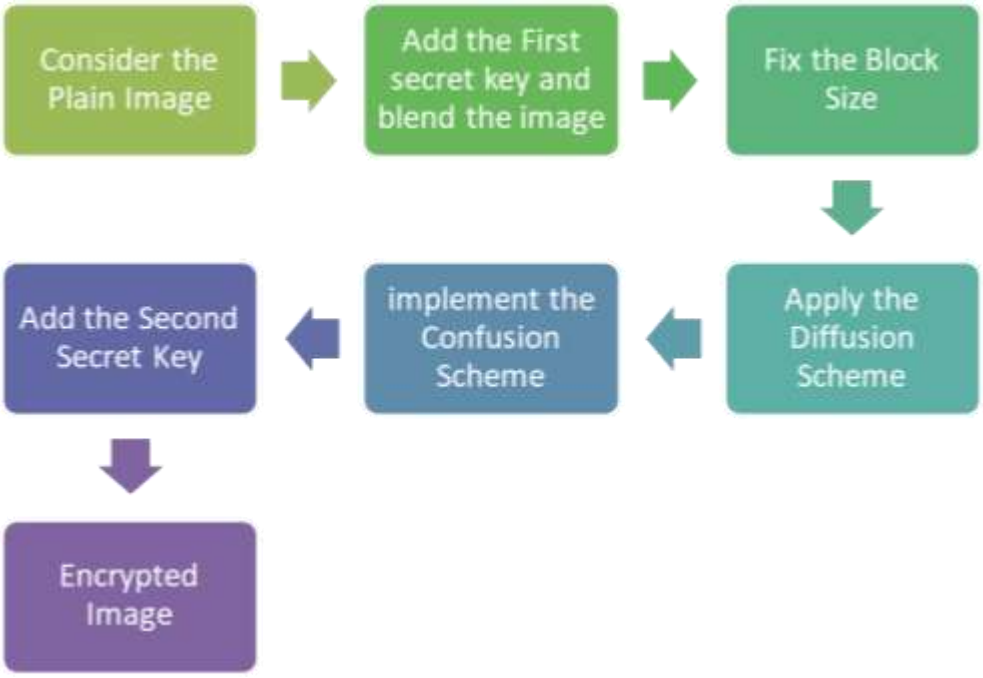


Figure 2 .Encryption Procedure

3.3 PERMUTATION PROCESS

A process known as "stage" is used to alter the pixels in every square within the same piece in order to disrupt the firm connection between the pixels. As an alternative, the partially encoded image is subjected to security calculations, such as those based on SCAN, before being processed. Both raster and zigzag patterns are common in SFC. As shown on a raster scan display, the raster SFC is a common method of checking that filters the image column by line. As shown in zigzag scans, SFC crisscrosses a picture through a neighbor's driving inclination. The current approach involves rearranging the pixels through the use of a zigzag scanning method. However, there are a few drawbacks to this approach. The

first is that this technique can only be used with square images. Secondly, there is a low encryption rate and a lengthy scanning process. Therefore, the saw tooth spacing filling curve (SFC) was suggested as a solution to these drawbacks..

3.3.1 Algorithm For Saw tooth SFC Technique

- The new SFC approach takes the output of the mixing technique as input.
- The secret key determines where to begin navigating the block.
- The input block can be scanned using adjacent sub-key pairs.
- When every set of sub-keys is used up, the process starts over from the first one.
- Finding the sub-key pair that navigate a certain piece is quite challenging.
- At long last, we have the encrypted picture.

3.4 Key Generation:

As a sophisticated public key cryptography algorithm, key generation (KG) is worth mentioning. A public key and a secret key are utilized by KG. To make the original images unintelligible, the open key is utilized for encryption.

The encrypted pictures can be deciphered using the secret key.

The following procedures can be used to create the open key and private key pair in this situation:

- Please create a large set of randomly generated prime numbers m[x, y] and n[x, y].
- A modulus n register is defined as s[x, y] = m[x, y] * n[x, y].
- Pick a non-prime odd integer between '7' and n-1 that is close to m-1 and n-1.
- Using e, m, and n, record the private illustration d.
- The public key is (s, e), while the private key is (s, d).

Key exchange remains an unresolved issue with the current methodology, which employs symmetric key encryption for both encryption and decryption. One solution to this issue is the use of asymmetric key cryptography. While the open key (s, e) is used for the mixing process and the private key (s, d) is used for the unscrambling process, KG is primarily used to communicate the secret keys in this work. A higher encryption rate is achieved using this method by using two separate keys.

3.5 Confusion Scheme:

One of the connected pixels in each square is used to alter the component's characteristics in this method. As shown in Figure 3, the selected adjacent pixel is one of the eight available nearest ranges, denoted as headings P1– P9.

.

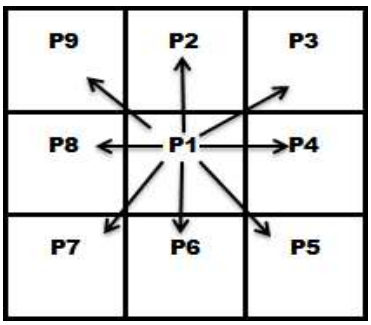


Figure 3 .Confusion Scheme

Algorithm:

- Sub-images of a partially encrypted image are broken down into 3*3 or 5*5 blocks.
- By exchanging the current element with its neighbor, the attributes of the present pixel are changed.
- To improve the security of both encryption and decryption, the confusion & inverse confusion technique uses two separate keys.
- The image is encrypted when the pixel properties of each piece are altered one by one, column by column.

3.6.Proposed Algorithm

Proposed SAIC encryption algorithm includes the following steps:

1. The KG algorithm produces two distinct keys.
2. The quality of the original image is diminished as the input image is relayed through the mixing process.
3. The partially garbled image is separated into parts that do not cover each other.
4. How many parts there are in total depends on how big the final picture is.
   Sub-key pairs (kx, ky) are used to further distribute the encoded picture.
5. To obtain the garbled image, this process is used for the saw tooth gap filling bend technique.
6. To obtain the final garbled image, the perplexity technique further prepares the mixed picture.
7. A file is used to compose the scrambled squares that are the result.

Here is an important aspect of the proposed decoding calculation:

In the reversed request, the unscrambling calculation process is identical to the encryption operation. The Inverse mixing procedure, Inverse diffusion, and Inverse confusion approaches make up the Secured Asymmetrical Image Decipher algorithm. Let me walk you through the recommended decryption technique.

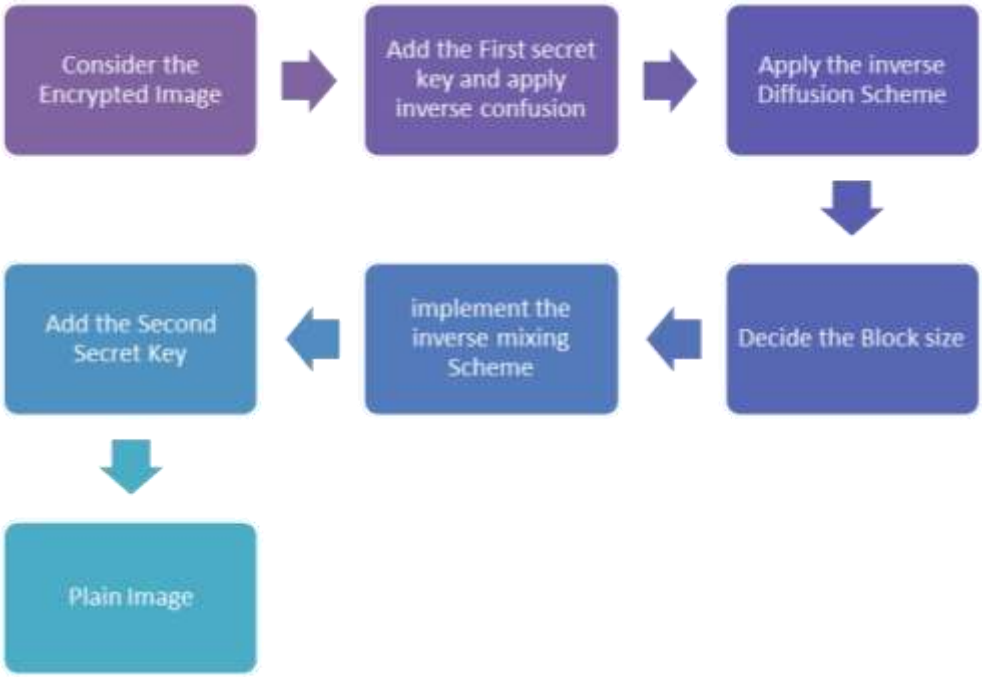


Figure 3 .Decryption Procedure

By applying inverse confusion and diffusion techniques to the encrypted image, we can decrypt it. In order to obtain the final decrypted image with the private key, the decrypted image is subjected to an inverse mixing procedure.

3.7 Dataset Used:

The USC-SIPI Image Database has been protected using our suggested Hybrid Asymmetric Image Cryptosystem (HAIC). For the purpose of evaluating encryption algorithms and image processing benchmarks, the USC-SIPI Image Database is second to none. Natural landscapes, aerial shots, textures, and classic grayscale photographs (such as Lena, Cameraman, and Barbara) are all part of the extensive collection. Image resolutions in the database range from 256×256 to 512×512, making it suitable for both low- and high-resolution encryption studies. These pictures are ideal for evaluating cryptosystems' statistical properties, diffusion, and confusion since they have varying degrees of texture, smooth regions, and high-resolution features. This dataset is frequently used by scientists for comparing encryption performance and checking parameters like entropy, correlation, NPCR, and UACI. Reproducibility and easy comparison with prior studies are ensured by its long-term use in image processing, which boosts the confidence in experimental results.

4. Experimentation and Results:

An ARM Cortex-M4/M7 MCU with at least 128 KB of RAM and at least 512 KB of flash is part of the test equipment for HAIC assessment, together with a desktop workstation running Intel i5 or i7 with 16 GB of RAM, Python 3.9, OpenCV, and PyCryptodome. Medical datasets such as NIH Chest X-rays or TCIA MRI scans, as well as benchmark images such as Lena, Cameraman, Baboon, Barbara, and Peppers, are used to offer both generic and healthcare-specific validation. To ensure statistical precision, tests are duplicated at least 30 times, and the system is constructed in Python/C using mbedTLS or OpenSSL for asymmetric primitives. While lossless decryption verifies accuracy, NPCR, UACI, entropy, histogram uniformity, and adjacent-pixel correlation evaluate security. We measure the MCU's performance in terms of things like encryption/decryption time, memory, throughput, and energy consumption. Decryption quality is evaluated using PSNR and SSIM, while robustness testing includes simulations of compression, noise, & packet loss. To demonstrate how much better HAIC is at security and efficiency, we compare its performance to baseline methods (such AES-256-CBC with RSA key exchange).

Our evaluation of the proposed HAIC is based on three criteria. Three factors have been assessed: key generation time, encryption time, and decryption time. Furthermore, we are contrasting our proposed HAIC with two existing schemes: QLog-CMD-AIE, which is based on asymmetric encryption with HCM in the frequency domain, and AC-HCM-FD-MIE, which is based on cyclic modulo diffusion algorithm. Table 1 below shows the results of our calculations for the three methods' encryption, decryption, and key generation times, with a key size of 512 bits as our baseline.

Table 1 Results of the Three Algorithms

Algorithms	Key Generation Time(ms)	Decryption Time(ms)	Encryption Time(ms)
QLog-CMD-AIE	487	526	605
AC-HCM-FD-MIE	331	402	487
HAIC	231	314	394

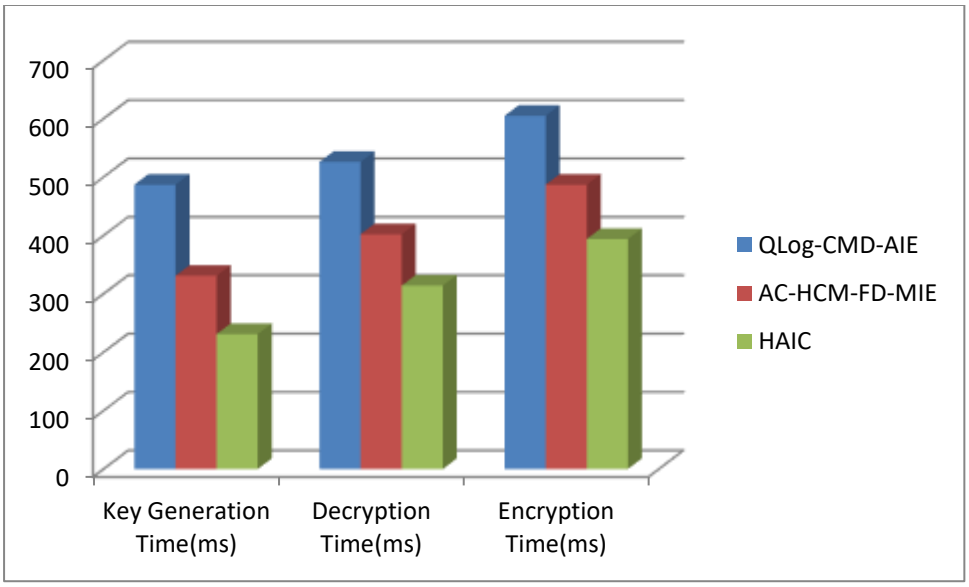
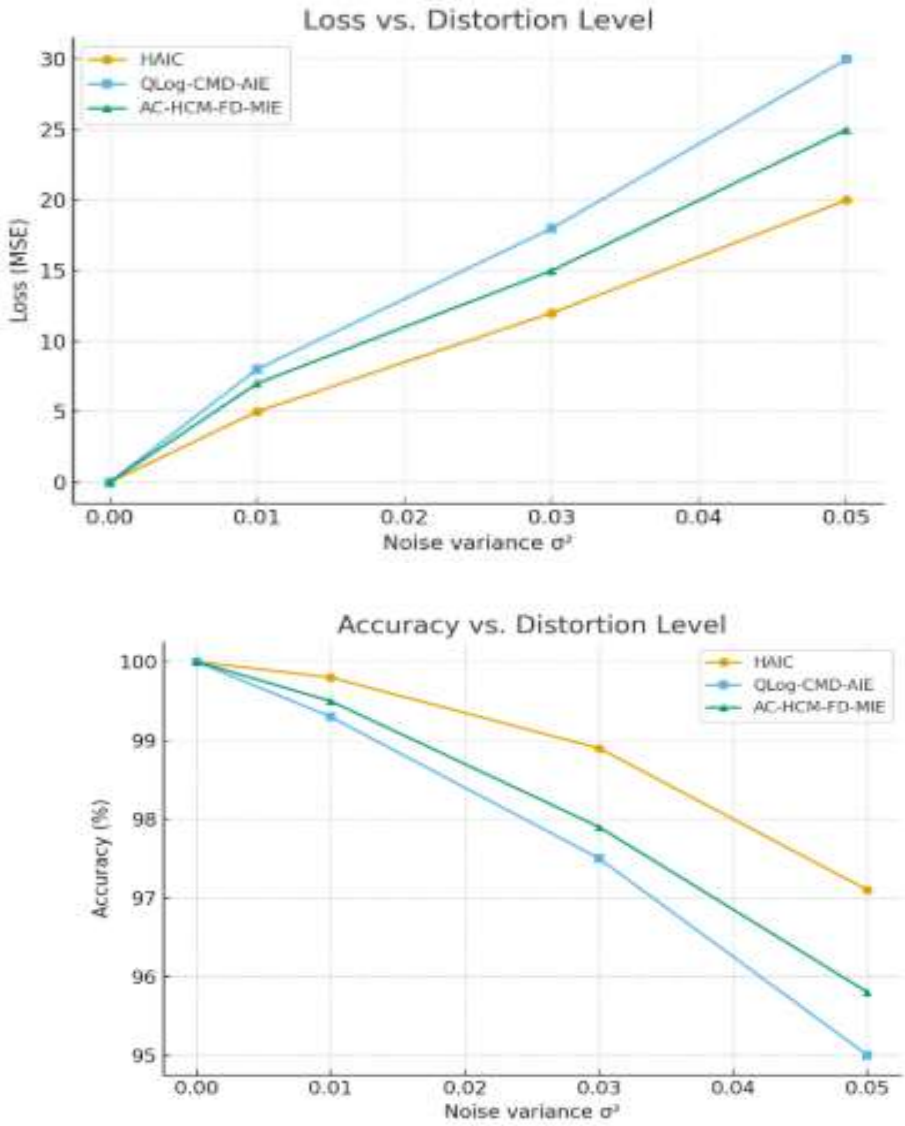


Figure 4 . Results graph of the three algorithms

Table 1 and figure 4 show that our suggested HAIC algorithm quickly provides an efficient key. In comparison to other watermarking cryptographic techniques, both the encryption time and the total encryption time are negligible. If these algorithms use mathematical functions and user assumptions to generate keys, the time it takes will grow. On all three occasions, the proposed method beats the state-of-the-art methods.

4.1 Accuracy and Loss Curves:

The below figures 5 & 6 shows the Accuracy and Loss Curves of the Proposed and existing algorithms.



Figures 5 & 6 Accuracy and Loss Curves of the three algorithms

In figures 5 and 6, we can see the results of comparing the three encryption methods AC-HCM-FD-MIE, QLog-CMD-AIE, and HAIC in the face of increased noise variation. In spite of extremely noisy conditions, HAIC maintains the best accuracy, as seen in the accuracy vs. distortion level curve, while QLog-CMD-AIE exhibits the steepest decline. The loss v. distortion level plot also shows that HAIC is more robust than QLog-CMD-AIE, with the lowest loss (MSE) across all noise values. When comparing accuracy and distortion robustness, HAIC typically comes out on top.

5. Conclusion:

This paper examines the several watermarking techniques, their features, their uses, and the most typical types of assaults that target photos with watermarks. This paper proposes a Secure Hybrid Asymmetric Image Cryptosystem (HAIC) Algorithm for pictures that makes use of an alternative method for the dissemination and replacement process; it is both simple and efficient. All the results that were discussed in the previous sections were obtained by using a single cycle, essentially. The nature of the application determines how many iterations are necessary to attain a better level of security. In order to make the suggested computation more robust against brutal power attacks, it should be possible to add further features, such as increasing the size of both the decryption and encryption keys. Suggested system is easily implementable in software and hardware. The approach is efficient, fast, and has a better order of security, therefore the approach can be employed in real practice. Asymmetric key systems, variable key spaces, keeping the file sizes of both the original & encrypted images unaltered, and utilizing logical operations for encryption and decryption are crucial elements of the proposed method. Because it uses

double watermarking to verify copyright, this approach enhances security while increasing the algorithm's runtime. We plan to improve the watermarking algorithm in the future so it runs faster without sacrificing resilience.

References:

1. P. Aberna and L. Agilandeeswari, "Digital image and video watermarking: methodologies, attacks, applications, and future directions," Multimed Tools Appl, vol. 83, no. 2, pp. 5531–5591, Jan. 2024,
2. D. K. Mahto and A. K. Singh, "A survey of color image watermarking: State-of-the-art and research directions," Computers & Electrical Engineering, vol. 93, p. 107255, Jul. 2023.
3. A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: a survey," Multimed Tools Appl, vol. 80, no. 20, pp. 30165–30197, Aug. 2023.
4. A. Bansal, B. Bhushan, S. Srivastava, "Wavelet-based robust and imperceptible watermarking for medical images", Multimed. Tool. Appl. 80 (4) (2021) 5397–5415,
5. V. Jaiswal, A. Sharma, "An improved robust watermarking scheme based on DWT and SVD for medical images", Journal of Healthcare Engineering (2022) 9321874,
6. H.A. Ali, H.H. Zayed, "Hybrid watermarking algorithm for securing medical images using DWT, DCT, and Logistic Map" J. Ambient Intell. Hum. Comput. 13 (2022) 2853–2865, https://doi.org/10.1007/s12652-021-03229-y.
7. J.C.M. Quintero, E.P.E. Cuesta, L.J.R. Lopez, "A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms", Results in Engineering 19 (2023) 101243, https://doi.org/10.1016/j. rineng.2024.102310.
8. S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Emmanuel, D.E.A. Mansour, L. Prokop, "Securing modern power systems: implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks", Results in Engineering 102647 (2024), https://doi.org/10.1016/j.rineng.2024.102647.
9. R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recogn. 34 (3) (2001) 671–683.
10. Y. Zhao, J.S. Pan, R. Ni, "Reversible data hiding using the companding technique and improved DE method" ,Circuits Systems and, Signal Process. 27 (2) (2007) 229–245.
11. P. Bedi, R. Bansal, P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance,"Comput. Electr. Eng. 39 (2) (2013) 640–654.
12. A. Amsaveni, P.T. Vanathi, "An efficient reversible data hiding approach for color images based on Gaussian weighted prediction error expansion and genetic algorithm", Int. J. Adv. Intell. Paradigms 7 (2) (2015) 156–171.
13. A. Amsaveni, C. Arunkumar, "An efficient data hiding scheme using firefly algorithm in spatial domain", IEEE Xplore (2015) 650–655.
14. Pan, J.-S.; Sun, X.-X.; Chu, S.; Abraham, A.; Yan, B. "Digital watermarking with improved SMS applied for QR code". Eng. Appl. Artif. Intell. 2021, 97, 104049.
15. Devi, K.J.; Singh, P.; Dash, J.; Thakkar, H.; Santamaría, J.; Krishna, M.V.J.; "Romero-Manchado, A. A new robust and secure 3-level digital image watermarking method based on G-BAT hybrid optimization". Mathematics 2022, 10, 3015.
16. Abdi, H.; Boukli Hacene, I. "An optimized medical image watermarking approach for E-health applications" Med. Technol. J. 2023,5, 594–603.
17. Hao, W.; Wei, X.; Zhang, W.; Xie, R. "Live code digital watermarking technology based on chaotic encryption". In Proceedings of the 2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Nanjing, China, 16–18 June 2023.
18. Anand, A.; Singh, A.K. "Hybrid nature-inspired optimization and encryption-based watermarking for E-healthcare. IEEE Trans. Comput. Soc. Syst. 2022, 10, 2033–2040.
19. Rai, M.; Hemlata. Robust digital watermarking based on machine learning. In Proceedings of the 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 18–20 October 2023.
20. Xiao, Y.; Xu, Y.-C.; Zhou, N.-R.; Lin, Z.-R. Digital watermarking scheme based on curvelet transform and multiple chaotic maps. Opt. Appl. 2023, 53, 291–305.
21. Kandi H, Mishra D, Sai SRK, Gorthi, "Exploring the learning capabilities of convolutional neural networks for robust image watermarking". Comput Secur 65:247–268,2019
22. Guo X, Yang W, Zhang L et al "Deep image watermarking with loss-driven modification. Multimed Tools "Appl. https://doi.org/10.1007/s11042-023-16809-5,2023
23. Hsu L-Y, Hwai-Tsu Hu, Chou H-H ,"A high-capacity QRD-based blind color image watermarking algorithm incorporated with AI technologies". Exp Syst Appl 199:117134,2022

24. Lee J-E, Seo Y-H, Kim D-W,"Convolutional neural network-based digital image watermarking adaptive to the resolution of image and watermark". Appl Sci 10(19):6854,2022
25. Mun S-M, Nam S-H, Jang H, Kim D, Lee H-K " Finding robust domain from attacks: A learning framework for blind watermarking". Neurocomputing 337:191–202. https://doi.org/10.1016/j.neucom.2019.01.067
26. Mahapatra D, Amrit P, Singh OP, Singh AK, Agrawal AK " Autoencoder-convolutional neural network-based embedding and extraction model for image watermarking". J Electron Imag 32(2):021604. https://doi.org/10.1117/1.JEI. 32.2.021604,2023
27. Fan Y, Li J, Bhatti UA, Shao C, Gong C et al " A multi-watermarking algorithm for medical images using inception v3 and DCT. Computers, Materials & Continua 74(1):1279–1302,2023
28. Nawaz SA, Li J, Bhatti UA, Shoukat MU, Li D, Raza MA "Hybrid watermarking algorithm for medical images based on digital transformation and MobileNetV2. Inf Sci 653:119810. https://doi.org/10.1016/j.ins.2023.119810,2024
29. Li, D., Li, J., & Bhatti, U. A. "Robust multi-watermarking algorithm based on darknet". In deep learning for multimedia processing applications (pp. 74–91). CRC Press,2024
30. Zhang W, Li J, Bhatti UA, Liu J, Zheng J et al "Robust multi-watermarking algorithm for medical images based on Googlenet and Henon map." Comput Mater Continua 75(1):565–586,2023
31. Balram, Gujjari, et al. "Application of machine learning techniques for heavy rainfall prediction using satellite data." 2024 5th International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2024.
32. Natarajan, V. Anantha, and M. Sunil Kumar. "Improving qos in wireless sensor network routing using machine learning techniques." 2023 International Conference on Networking and Communications (ICNWC). IEEE, 2023.
33. Rani, K. S., Jayadurga, R., Raja, V. L., Kumar, M. S., Swathi, R. S. V. R., & Kumar, P. (2022). Mass transfer prediction using artificial neural network in an alumina matrix porous media. European Chemical Bulletin, 11(11), 113-120.
34. Davanam, Ganesh, T. Pavan Kumar, and M. Sunil Kumar. "Efficient energy management for reducing cross layer attacks in cognitive radio networks." Journal of Green Engineering 11.2021 (2021): 1412-1426.
35. AnanthaNatarajan, V., M. Sunil Kumar, and V. Tamizhazhagan. "Forecasting of wind power using LSTM recurrent neural network." Journal of Green Engineering 10 (2020).
36. Balaji, K., Kiran, P. S., & Kumar, M. S. (2020). Resource aware virtual machine placement in IaaS cloud using bio-inspired firefly algorithm. Journal of Green Engineering, 10(2020), 9315-9327.
37. Godala, Sravanthi, and M. Sunil Kumar. "A weight optimized deep learning model for cluster based intrusion detection system." Optical and Quantum Electronics 55.14 (2023): 1224.
38. Suman, J. V., Mahammad, F. S., Sunil Kumar, M., Sai Chandana, B., & Majji, S. (2024). Leveraging natural language processing in conversational AI agents to improve healthcare security. Conversational Artificial Intelligence, 699-711.
39. Kumar, M. Sunil, and D. Harshitha. "Process innovation methods on business process reengineering." Int. J. Innov. Technol. Explor. Eng 8.11 (2019): 2766-2768.
40. Gandikota, Hari Prasad, Abirami S, and Sunil Kumar M. "CT scan pancreatic cancer segmentation and classification using deep learning and the tunicate swarm algorithm." Plos one 18.11 (2023): e0292785.
41. Ganesh, D., et al. "Improving security in edge computing by using cognitive trust management model." 2022 International Conference on Edge Computing and Applications (ICECAA). IEEE, 2022.
42. Kumar, M. Sunil, et al. "Crop yield prediction using machine learning." 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET). IEEE, 2023.
43. Kumar, M. Sunil, and D. Ganesh. "Improving telemedicine through IoT and cloud computing: opportunities and challenges." Advances in Engineering and Intelligence Systems 3.03 (2024): 123-135.
44. Kumar, M. Sunil, et al. "Enhancing Sentiment Analysis with an Attention Based Machine Learning Model." 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS). IEEE, 2023.
45. M. Jana and B. Jana, "A new DCT based robust image watermarking scheme using cellular automata," *Information Security Journal: A Global Perspective*, vol. 31, no. 5, pp. 1–17, 2021.
46. S. Helal and N. Salem, "A hybrid watermarking scheme using Walsh Hadamard transform and SVD," *Procedia Computer Science*, vol. 194, no. 1, pp. 246–254, 2021.
47. M. M. Eltoukhy, A. E. Khedr, M. M. Abdel-Aziz, and K. M. Hosny, "Robust watermarking method for

securing color medical images using Slant-SVD-QFT transforms and OTP encryption," *Alexandria Engineering Journal*, vol. 78, no. 2, pp. 517–529, 2023.
48. Z. Chen and G. Ye, "An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing," Optik, vol. 267, p. 169676, Oct. 2022
49. Y. Kumar and V. Guleria, "A novel multiple image encryption technique based on asymmetric cryptosystem with HCM in frequency domain," Multimedia Tools and Applications, vol. 83, pp. 72 253–72 278, Sept. 2024.