# INTERNATIONAL JOURNAL OF
## PURE AND APPLIED SCIENCE & TECHNOLOGY

# ON THE IMPLEMENTATION OF A SECURED WATERMARKING MECHANISM BASED ON CRYPTOGRAPHY AND BIT PAIRS MATCHING

1.DR S PRADEEP,2. K. PRANVITHA,3. V. SAILAXMI,4. K. SREEJA RANI,5. USHASWINI

**ABSTRACT:**
Watermarking is one of the most vital digital information hiding technique, which can be used with cryptography mechanism for providing more security to digital data. In image watermarking mechanism mostly LSB substitution is used on the cover image for hiding the secret watermark. In this paper, a novel technique based on the matching of bit pairs and symmetric key cryptography is proposed. Pixel bits of original image and encrypted watermark image are arranged in pairs. The pixel bits are represented in pairs following the proposed algorithm, then the encrypted watermark pixel bit pairs are compared with all bit pairs of original image and accordingly the replacement of bit pairs takes place with the respective matched pair assigned number binary equivalent. If no match is found then go for replacing the 0th pair with watermark bits and replace the two LSB with the value of pair number 0. The proposed mechanism shows good quality of watermarked image along with good PSNR values with a good payload. By comparing the results with some existing algorithms, the proposed scheme shows the valuable results.

## INTRODUCTION

For copyright protection of multimedia information, a variety of digital watermarking techniques have been developed, which are used to protect the multimedia information from being abused. There are two categories of techniques of embedding the water-mark for copyright shield in any multimedia information, be it the image, audio or video. The spatial domain technique follows any particular algorithm for embedding of the watermark by directly adding it to the data, and the frequency domain method is to embed it in any of the transform domain. The spatial domain of watermarking is faster but fails in robustness while the frequency domain watermarking is robust but still consumes more resources in terms of power consumption and slower speed of computing (Acken, 1998; Low et al., 1998; Macq and Pitas, 1998;Swanson et al., 1998).It is better to go for the higher cost of computing to get the benefits of robustness of the watermark when maliciously attacked by the mechanisms of noise, filtering or compression. For the realization of the watermarking mechanisms, the major areas of focus are imperceptibility, robustness, capacity, security, and trustworthiness. The perceptual transparency of the hidden data or information is the imperceptibility.

**1.PROFESSOR&HOD,2,3,4&5 UG SCHOLAR**
**DEPARTMENT OF IOT, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD**

Survival of the watermark information against intentional or unintentional attacks without significant degradation of the quality of the original image is the robustness. The payload for the new signal is defined as the capacity and the undetectability of the watermark information on the corresponding media, which is defined as the security and all these turned to be very important considerations in case of invisible-watermarking (Liu and Tan, 2002; Zhu et al., 2006; Gutab and Ghouti, 2007). A well-known survey of watermarking techniques can be found from (Kutter and Hartung, 1999; Mohanty, 1999;Altaibi et al., 2015). There is a trade-off between these parameters as an increase in robustness may appear at the expense of enhanced watermark signals visibility as well as reduced band-width. But, the perceptual distortion of the image, due to water-mark embedding is not related directly to the magnitude of the watermark signal. It can be observed that the watermark signal of same strength is causing less visual distortion in busy areas of the image than the flat background. In the papers (Podilchuk andWenjua, 1998; Hannigan et al., 2001) on watermarking, there is less effort to evaluate images in order to consider the upper limit of the power of the watermark signal without considerable visual distortion. These spatial domain methods neglect the significance of payload capacity and mostly focused on the imperceptibility factors. In Khan and Gutub (2007) the authors proposed an image based message concealment mechanism by use of punctuation marks to encode a secret message and by using modified scytale cipher provides the better result as far as the security is concerned. In Al-Otaibi (2014) the author proposed a data hiding technique with two layers of the security system by including AES cryptography followed by image-based steganography to ensure high security. Methods of LSB matching is proposed in Sharp (2001), which also called ± embedding mechanism (Li et al., 2011). In this method, the cover image pixel value is increased or decreased randomly by one when the secret bit is not equal to the LSB of the pixel belonging to the cover image (Huang et al., 2014). The LSB-M modifies both the histogram of an image and the correlation-between the adjacent pixels, which helps the steganalysis methods to attack this method (Xia et al., 2016). In Sabeti et al. (2013) the authors proposed complexity based LSB matching scheme, where the LSB matching is used in order to enhance the security against possible attacks. This mechanism uses a local neighbor hood analysis to determine the secure locations of an image and then LSB matching used for the embedding process. In Parvez and Gutub(2011) the authors proposed one image steganography algorithm, which determines the number of secret message bits that each pixel of the cover image can store based on a partition scheme of color intensity range. This scheme provides high data hiding capacity and security for the host image

**RELATED WORK** A comprehensive survey on RDH is presented by Shi et al. [11] to deeply analyze and highlight the advances of RDH for the recent progress. It studies aspects of RDH, including RDH into image spatial domain [1, 2], RDH into image compressed domain (e.g., JPEG) [12, 13, 14], RDH suitable for image semi-fragile authentication [15, 16, 17], etc. In particular, it also investigates RDHEI, and categorizes the existing RDHEI schemes into two classes: vacating room before encryption and vacating room after encryption by embedding strategies. For key setting, Shi et al. [11] also mentioned the other notion, so-called RDHEI based on public key encryption. However, inspired by the factor of key setting, the

present studies identify the following two notions of RDHEI.1 • Share independent secret keys (SIK). R shares independent keys, keyP and keyH, with P and H respectively. Notably, these keys (keyP , keyH) are secret and used to run image encryption and embedding algorithms. Numerous insightful works [10, 18, 19, 20, 21, 22] have proposed this type of RDHEI schemes. • Share no secret key (SNK). In contrast to SIK, R does not need to share any secret key. This can be easily achieved through public key encryption where R has a public/secret key pair, and P (H, resp.) can use the public key to do image encryption (data embedding, resp.). The first solution, proposed by Chen et al. [23], is to use Paillier homomorphic encryption [24] to encrypt each pixel and rely on specific techniques to complete data embedding. With the use of the homomorphic encryption, the follow-up works of Zhang at al. [25], Li and Li [26], and Shiu et al. [27] respectively implement some reversible data hiding techniques under the public key encryption associated with the homomorphic property. To summarize the flexibility of key setting, it is clear that only the designated party who has the secret key can be P or H in SIK. However, the advantage of SNK is that anyone can be P or H, since the keys of encryption or embedding are exactly the public key. In addition, as known, those homomorphic encryption-based SNK-type RDHEI schemes are practically inefficient since the underlying encryption schemes usually rely on complicated algebra structures and spend high computational cost. It suffices to give the following question, and we will aim for addressing it in the remainder of this paper. Can we construct an efficient scheme to satisfy the intermediate notion (between SIK and SNK) where P and R share a secret key, but no secret is shared with H? In fact, Wu et al. [28] had proposed a shared one key (SOK) scheme based on secret sharing. However, their method spends much space cost, since it encrypts a pixel into n shares,

where n is the security parameter of secret sharing, and the total cost of an encrypted pixel will blow up to 8n bits.

## IMAGE STEGNOGRAPHY

Image steganography comprises of transform domain, model relied steganography, spatial domain and spread spectrum. The spatial domain and transform domain contrasts with one another. Pixel value is directly used to embed a secret message in spatial domain. On the other hand, transform domain techniques accomplish embedding by initially transforming the particular image from STF (Spatial to Frequency) domain via the use of any of the mentioned transforms. They are DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform), Ridgelet Transform, Hadamard Transform, DD DT DWT (Double Density Dual Tree DWT), Dual Tree, Curvelet Transform and so on. Then, embedding is performed in specific transform-coefficients. The recent progress in the communication and information technology generates easy and simple accessible data. In addition, establishing secure communication is the most important requirement. Various methodologies are generated to accomplish safe communication. One such methodology is steganography.

Steganography consists of four modules. They are listed below.

- ➢ CO (Cover Object) – Data hiding is performed in this CO.
- ➢ SD (Secret Data) – Within the CO, the hidden-data is positioned.
- ➢ SO (Stego Object) – state of CO after the data is hidden inside.

- ➢ SK (Stego Key) – Hide function is used for the hidden data within the CO.
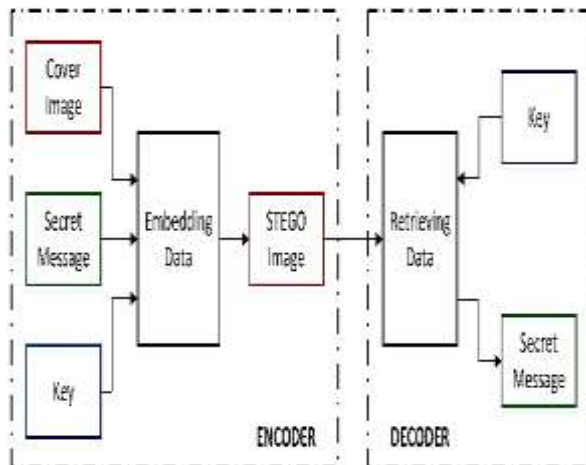
**Figure.1. Fundamental steganography architecture**

In the above figure.1, the cover image, secret message and key is used for embedding the data to attain the stego image. This is done is the encryption phase. In contrast, the secret message is retrieved by using the key in the decryption phase.

## EXISTING SYSTEM

➢ LSB embedding position, and encrypt the message which control embedded position, so the hidden information cannot be extracted without the corresponding private key.

➢ In order to prevent the forgery of the hidden information, A text segmentation method is performed which attempts to extract the text.

➢ The proposed pre-processing method improves crop image performance.

➢ RC4 algorithm using Encryption key Generation

## DISADVANTAGES

➢ High Encryption and Decryption Time.

➢ The key Generation is poor.

➢ It doesn't hidden data is extracted by the receiver through the reverse process.

➢ It is doesn't validate its performance efficiency.

## PROPOSED SYSTEM

In proposed several techniques to accomplish image steganography. Initially, the image is taken as input and pre-processing is performed by using the Pixel Repetition Method. In the pre-processing technique, various unwilling distortions are suppressed and the significant image features are used for further processing. Then, recommended AES cryptosystem is used for data encryption. This process helps in achieving communication security. Proposed new LSB embedding is utilized to hide the secret data inside an image. Finally, the hidden data is extracted by the receiver through the reverse process of the A* Algorithm proposed system. The proposed system in analyzed to validate its performance efficiency.

## ADVANTAGES

➢ Low Encryption and Decryption Time.

➢ It will Key Generation easy for AES algorithm.

➢ It hidden data is extracted by the receiver through the reverse process using A* algorithm

➢ It is based on analyzed to validate its performance efficiency.

## LITERATURE REVIEW

**Title**: Image Steganography with Artificial Immune System

**Year**: 2017

**Author**: Saleh Delbarpour Ahmadi, Hedieh Sajedi

**Methodology**

Selects a block of the host image and then employs AIS for finding the best template for embedding message bits in the host image pixels. Consequently, our method finds the best template for embedding rapidly and there is no need to investigate whole the image for finding a template of embedding. Algorithm has more efficiency in term of embedding capacity and the time of the embedding process compared to other methods.

**Advantage**

➢ It has more efficiency in term of embedding capacity

**Disadvantage**
- It requires High Cost
- It is Low Encryption and Decryption Time

**Title**: Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm
**Year**: 2018
**Author**: De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto
**Methodology**
Steganography domains coupled with Cryptography which aimed to make confidential information more secure and inaccessible to unauthorized persons. Messages are encrypted using the 3-DES side of the cover image is decomposed into using LSB method. The last step, done Inverse DWT (IDWT) to get the stego image.
**Advantage**
- Image is decomposed into using LSB is Fastly Hidden

**Disadvantage**
- Encryption and Decryption Time is high.

**Title**: Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques
**Year:** 2018
**Author**: Ahmed Hambouz, Yousef Shaheen, Abdelrahman Manna, Dr. Mustafa Al-Fayoumi, and Dr. Sara Tedmori
**Methodology**
This research paper introduced a new steganography technique that achieves both data confidentiality and integrity. Data confidentiality is achieved by embedding the data bits in a secret manner into stego image. Integrity is achieved using SHA 256 hashing algorithm to hash the decoding and encoding variables.
**Advantage**
SHA 256 hashing algorithm to hash the decoding and encoding.
**Disadvantage**

Drawback of Time and Cost.

**Title**: A new image steganography method with optimum pixel similarity for data hiding in medical images
**Year:** 2020
**Author**: Songul Karakus, Engin Avci
**Methodology**
Data hiding capacity and image quality of the cover object are important factors in image steganography. Because the deterioration of image quality can be noticed by the human vision system, it attracts the attention of attackers. Therefore, the purpose of this study is increasing the amount of data to be hidden and stego image is to ensure high image quality.
**Advantage**
- It is based on High Resolution Image

**Disadvantage**
- Drawback Of Time and Cost
- Performance Analysis is a varying.

**Title**: Adaptive Image Steganography based on Transform Domain via Genetic Algorithm
**Year:** 2017
**Author**: Aref Miria and Karim Faez
**Methodology**
This paper presents a novel approach for data hiding in frequency domain with the use of genetic algorithm. At first, cover images are mapped to a proper frequency domain using the concepts of adaptive wavelet transform and genetic algorithm. In the obtained space, using a model based on Kieu and Chang, encrypted information will be embedded in the frequency coefficients that represent edges of the image in spatial domain. So the cover image will change the least and have the most compatibility with human visual system. Simulation results show that our proposed method outperforms recently

published works in terms of PSNR and PSPNR factors.

**Advantage**
It is possibility to get prediction of local differences between images (on the pixel level), while methods described previously provided a single value for the entire image.

**Disadvantage**
VDP is non-use information about color, and work only with brightness.

**Title:** A Study of Various Steganographic Techniques Used for Information Hiding
**Year:** 2013
**Author:** C.P.Sumath, T.Santanam and G.Umamaheswari
**Methodology**
In this paper different steganographic articles were studied and were categorized into different techniques. As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing application areas also.

**Advantage**
➢ Steganography is to embed secret data into a cover in such a way that no one apart from the sender and intended recipients even realizes there is secret data.

**Disadvantage**
➢ There is large overhead to hide very tiny amounts of information.

**Title**: Chaotic Map Based Random Image Steganography Using LSB Techniqu
**Year**: 2017
**Author**: Sujarani Rajendran, Manivannan Doraipandian
**Methodology**

A new chaotic series based image hiding scheme has proposed by using 1D logistic map. Cover image pixel position has chosen randomly for embedding the secret image bits, so it minimize the security risk and increase the efficiency of the proposed algorithm. Four different grayscale images are used for testing to prove the performance, image quality and capacity of the proposed scheme. Comparison result proved that the proposed scheme provide better result than other steganography schemes.

**Advantage**
➢ Over cryptography alone, is that messages do not attract attention to themselves.

**Disadvantage**

➢ Text files cleanly aren't big enough to cover more complex data like images or audio files.

**MODULES**
➢ Input Image
➢ Pre-processing
➢ AES Cryptosystem
➢ Extract the Hidden Data
➢ Performance Analysis

**MODULES DESCRIPTION**
**INPUT DATA**
➢ The data selection is the process of selecting and loading the input images from dataset.
➢ The dataset is used to Secret text from the input text.
➢ To read the image with the help of imread() function.

**DATA PREPROCESSING**
**Pixel Repetition Method**
➢ The image taken as input is scaled-up by the use of PRM (Pixel Repetition Method). The (X*Y) input image is scaled-up by converting the individual pivot or seed pixel into a block (2*2) by reiterating the pixel. Thus, a cover is generated with twice the input image dimensions given by (2X*2Y). The C (2X*2Y) is the CI

(Cover Image) acquired from the input image.

➢ A (2*2) original image block is considered. Then, the scaled-up image is retrieved as shown in the below figure.3.
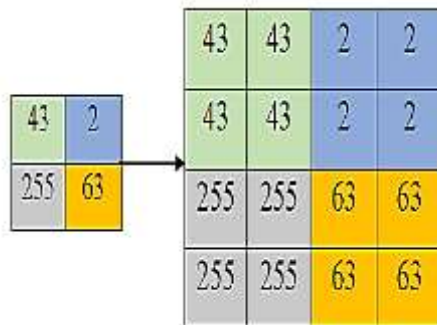


➢ Every pivot or seed pixel is reiterated to attain 2*2 blocks. Thus, it is termed as PRM (Pixel Repetition Method). The use of PRM to perform pre-processing minimizes the computational-complexity.

## AES CRYPTOSYSTEM

➢ The AES (Advanced Encryption Standard) is a cryptographic-algorithm utilized for textual data encryption in an unconceivable way. It is also called as symmetric-key algorithm. This indicates that similar key is utilized for encryption as well as for decryption. It also utilizes block cipher that are of varied sizes. In recent days, AES is supported in software and hardware and hence it is a robust security algorithm. In addition, AES has various merits. They are listed below:

➢ The built in key length flexibility permits an extent of future proofing in contrast to the advancement in the capability for performing EK (Exhaustive Key) searches.

➢ This algorithm is robust against attacks as it utilizes high key size length of 128, 192 as well as 256 bits for the encryption process. Till now, there exists no real world cryptanalytic-attacks are discovered when using AES.

## LSB EMBEDDING

➢ In this technique, the LSB (Least Significant Bits) of few or all the bytes within an image is substituted with a bits corresponding to the secret message. This method can be employed to various types and formats of data. Thus, this technique is the significant steganography method now-a-days. This technique is susceptible to steganalysis. Hence, the raw data is encrypted prior to embedding process to achieve more security. This approach has turned out to be the basis of various methods that hide the messages within the MCD (Multimedia Carrier Data). This can also be employed in specific data domains. For instance, a hidden data is embedded into the RGB bitmap data colour values or into the JPEG image frequency coefficients. The fundamental steganography method is LSB. Here data is presented into the pixels of the cover image directly. This methodology has efficient recognizable value. Thus, normal people are unable to identify the alteration in an image. By modifying the LSB bit-plane, the insertion process is undertaken for individual pixel. This methodology has various merits. They are listed below.

➢ It is simple to comprehend.

➢ It provides easy implementation.

➢ It affords stego images which consists of hidden data, yet seems to have more visual fidelity.

➢ Least Significant Bit Steganography or LSB Steganography is the method of hiding secret data inside any form of digital media, here, Image. Images are made up of pixels which usually refer to the color of that particular pixel. In a grayscale image, these pixel values range from 0-255, 0 being black and 255 being white. In LSB Image Steganography, changing the last bit value of a pixel, won't have much of a visible change in the color. A cover

image is used to embed the data in. The otput of the process is called a Stego Image

➢ To embed a message in an image using LSB Steganography the following steps are involved: The Cover Image is converted to greyscale. The message is converted into binary. Each pixel of the image is traversed through, and for each pixel, initiate a temporary variable, temp.

If the LSB of the Pixel Value and the message bit are the same, set temp as 0 and set temp as 1 otherwise. Update the output image pixel as image pixel value added with the temporary variable value, temp.

This is done until the message is completely embedded. Once the whole message is embedded, the output image us written.



.
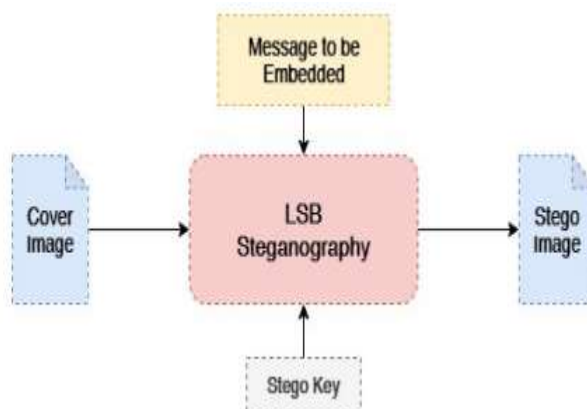
**Extract the Hidden Data**
➢ In Cover Image hidden text Retrieval
➢ It affords stego images which consists of hidden data, yet seems to have more visual fidelity

**A*Algorithm**
➢ Informally speaking, A* Search algorithms, unlike other traversal techniques, it has "brains". What it means is that it is really a smart algorithm which separates it from the other conventional algorithms.
➢ This fact is cleared in detail in below sections. And it is also worth mentioning that many games and web-based maps use this algorithm

to find the shortest path very efficiently (approximation).

**RESULT GENERATION**
The Final Result will get generated based on the overall performance of this proposed approach is evaluated using some measures like,

**PSNR**
Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of an image and the power of corrupting noise that affects the quality of its representation.

**MSE** MSE is used to check how close estimates or forecasts are to actual values. Lower the MSE, the closer is forecast to actual. This is used as a model evaluation measure for regression models and the lower value indicates a better fit.

**CONCLUSION**
In this process, Image Encryption and Decryption Process. Image is taken as input and pre-processing is performed by using the Pixel Repetition Method. Various techniques are used to achieve image steganography through encryption and decryption. Pixel Repetition Method is used to perform pre-processing. Later, proposed AES system is used to encrypt the data and LSB embedding is utilized for embedding the data thereby performing image enhancement through the so as to extract the hidden data. To perform on analyzed to validate its performance efficiency.

**FUTURE ENHANCEMENT**
Various techniques are used to achieve image steganography through encryption and decryption. Pixel Repetition Method is used to perform pre-processing. Later, proposed AES system is used to encrypt the data and LSB embedding is utilized for embedding the data thereby performing image enhancement and pixel adjustment through the proposed novel OPAP based CNN so as to extract the hidden data. Many Algorithm using Society wise uses on Application.

**REFERENCES**

➢ S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," Medical Hypotheses, vol. 139, pp. 109691-109691, 2020.

➢ C. Y. Roy and M. K. Goel, "Visual Cryptographic Steganography with Data Integrity," Lovely Professional University, 2017.

➢ P. Rahmani and G. Dastghaibyfard, "An efficient histogram-based index mapping mechanism for reversible data hiding in VQ-compressed images," Information Sciences, vol. 435, pp. 224-239, 2018.

➢ M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

➢ N.Latha1, N.Dharani2, M.Nithya3, Mr.S. Srikanth4, Spying Robot With Camera Rotation For War Fields, International Journal For Recent Developments In Science & Technology , Issn: 2581-4575,Volume 06, Issue 11, Nov 2022,Pg 19-22

➢ S. D. Ahmadi and H. Sajedi, "Image steganography with artificial immune system," in 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017, pp. 45-50.

➢ S. Karakus and E. Avcı, "A New Image Steganography Method wıth Optımum Pıxel Sımılarıty for Data Hıdıng ın Medıcal Images," Medical Hypotheses, p. 109691, 2020.

➢ A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," Optik, vol. 145, pp. 158-168, 2017.

➢ M. Umair, "Comparison of Symmetric Block Encryption Algorithms," ResearchGate, 2017.

➢ A. K. Sahu and G. Swain, "A review on LSB substitution and PVD based image steganography techniques," Indonesian Journal of Electrical Engineering and Computer Science, vol. 2, pp. 712-719, 2016.

➢ L. Laimeche, A. Meraoumia, and H. Bendjenna, "Enhancing LSB embedding schemes using chaotic maps systems," Neural Computing and Applications, pp. 1-19, 2019.