Privacy Preserving On Remote Sensing Data Using Reversible Data Hiding

K Saravanan1,3,4, K Suganthi2,3,4, R Kalaiselvi2,3,4, B Divya2,3,4 and S Dilip Kumar2,3,4

PG Scholar1, Assistant Professor2
3Department of Computer Science and Engineering
4Arasu Engineering College, Kumbakonam, Tamilnadu, India

shravanan560@gmail.com1, pksuganthi@gmail.com2, kalaiprathi85@gmail.com3, dhivyabaskar91@gmail.com3, sdilipkumar85@gmail.com4.

Abstract. The method of steganography covers message in the cover file and forms a stego file. Imagery needs a method that will boost protection, minimise distortion in the stego file and recover data without failure. There is a need for reducing transmitting time in the age of multimedia and the Internet. The main purpose of this project is to create safe contact between the sender and the recipient through emails and other modes of communication. A reversible data hiding algorithm was proposed in the integer wavelet transformation (IWT) domain to resolve the image distortion problem. This strategy aims to incorporate data into IWT coefficients of higher frequencies. After wavelet coefficients are collected by converting the integer wavelet data into high-frequency subbands HL, LH and HH, the human eyes would have fewer recognisable objects. After data is incorporated in such IWT coefficients, reverse integral wavelet transformation can occur following application. The stego image was further encrypted by using Elliptic Curve Cryptography (ECC). The process of encryption enhances the image security during data transmission. In our proposed work inverse wavelet transformation (IWT) and Elliptic Curve Cryptography (ECC) algorithms are effectively utilized to achieve highly secure communication.

Keywords: Elliptic Curve Cryptography; Integer Wavelet Transformation; Reversible Data Hiding; Grey Wolf Optimization; Least Significant Bit; Media Content Server.

1. Introduction:
Reversible Data Hiding (RDH) is an intermedia technology that enables users to integrate further details into the cover picture. The receiver side also ensures that after the embedded data is separated from the identified picture the cover image can be retrieved losslessly. RDH plays an important part in certain delicate situations in medical imaging, forensics, remote sensing images, material authorisation[1-2], where any distortions on cover media or extra evidence on the receiving side cannot be accepted. There are several RDH strategies which can be narrowly separated into three categories: extension of discrepancies [3], bar chart change [4] also, lossless pressure [5]. Fundamentally two measures are used in RHD techniques. The first step is to produce a low-entropy host graphic, for example the host has a sharp histogram that can normally be achieved applying a forecasting bug coupled with the categorizing method [6]. The assisting stage reversibly integrates the extra information into the host picture.

In the latest Cloud growth, Clients can conveniently deploy their cloud data, but Clients seek the
protection of their files across the Cloud in certain sensitive scenarios. Users can scramble the media document previously they upload to the cloud server to preserve the privacy of the multimedia Directory. For the purpose of cloud-based file management, the cloud owner or channel manager has to embed any additional messages in the encrypted file without knowing the original content of the Multimedia File utilising protected cloud preparing like starting point data, sight and sound record documentation or verification details. The cloud [7–10] takes advantage of this feature of embedding additional messages in encrypted files. For instance, a database controller may enclose sensitive details into the accompanying encrypted photos if a patient is to be encoded because of protection issues. The original text is therefore error-free after decryption and the user will find additional message (patient personal information).

Encrypted Picture Reversibility Data Hiding (RDHEI) fulfils this prerequisite and has the same features. RDHEI needs to insert new details into an encrypted picture when reconstructing the initial image and retrieving additional information from the user. The concept comes from the RDH which ensures that the original image is restored without loss after abstraction of extra details from the checked picture. This capability is supported more efficiently by our framework. For encrypted photos the classic HDR algorithms are not suitable. Many researchers therefore demonstrate their worry about the creation of RDH in encrypted pictures.

In [7] it is suggested that the first RDHEI algorithm be used to re-install more data using LSBs. The stream cipher is used in initial image encryption, although pixel correlation statistics are taken into consideration for full image recuperation at the recipient end following direct image decryption. In [11] the improvement of [7] by side match technology is suggested. Additional details from the decryption of uploading photos may be retrieved, which ensures a client has to have both a masking and encryption key. These algorithms are of a type that cannot be isolated. The separable RDH system was suggested by Zhang in [12]. The recipient may use this approach to access additional data with the hiding key, independently of the decryption activity. [13] Qian et al. suggested a means of integrating additional data in an encrypted image utilising a histogram adjustment and n-array data hiding framework. The integration and accuracy of the image were improved with that process, but the image protection was diminished by image histogram leakage. The encrypted picture has been compressed by Zhang and others [14], using the LDPC to inject the compressed images. The noisy series of picture encryption by Zheng et al. [15] has been compressed using Hamming Distance to compact the pixel LSBs. The content evaluation of the direct decrypted picture involves prioritisation, and the ability of both Puyang et al.[16] and Xiao et al.[17] to incorporate into the encrypted image is large. Other papers presented include encrypted images of pallets in [18], description of picture blocks and allowance in [19]. The solutions above are focused on symmetrical encryption systems, such that key storage on the cloud personal network does not function effectively.

2. Related work:

The plan to use Grey Wolf Optimization (GWO) and Convolutionary Neural network (Garg, Sahil et al.)[20] to implement a hybrid data management platform for network anomaly detection is (CNN). The GWO and CNN learning methods were updated to increase the potential of the proposed model: (i) improved exploratory, exploitative, population-generating and (ii) revised dropout features. The comprehensive versions are referred to respectively as enhanced-GWO (ImGWO) and enhanced CNN (ImCNN). Tcpdump logs are derived from these data sets since they comprise primarily traffic details for the CC infrastructure. These logs contain TCP and UDP packets that comprise almost 90 per cent of data center traffic. In the second step, this model processes the input data for ImGWO to reflect network traffic data. TCP and UDP packets from tcpdump logs are extracted and are provided as an IMGWO input.

The related shared media infrastructure system for the effective co-operation of health care staff is
presented by Hossain et al. [21]. The therapy frame for patients with voice pathologies is specially built. The smart phone, used as a media sensor, will give a patient their voice. The MCS gets and sends it to Cloud Manager Media content server (CM). The CM transmits speech details to the CSM and the CSM uploads information to the website for family doctors. The CSM offers servers to delete features from the voice, model regular or abnormal samples, and categorise the samples. The doctor then prepares a report and sends it to the CSM after reviewing the information. The report will be collected by the physician by proper automation if the family practitioner may review the report by other physicians. The article can be analysed and his suggestions posted. Then it is collected and deposited in the CM in the CSM. The doctor will provide the patient with the input from the CM. The consistency during transmitting of the voice is a crucial issue in this relationship between patients and physicians, as pathologic voice is already loud.

Introducing a trust-based multimedia analytics model, Garg et al. [22] is eager to satisfy growing demands of consumers and to have a timely, operable perspective. Software Defined Networks are of crucial significance in this respect but a range of considerations, for example the protection of runtime and energy-awareness networking are restricting its capacities for effective network management and control. In order to increase the efficiency of SDN it is therefore suggested a hybrid deep learning anomaly detection method in the sense of social multimedia for suspicious flow detection. There are two devices, (2) a Boltzmann Computer and Gradient Descent-based Support Vector Machine for anomaly detection module for detection and and, (2) an End-to-end module for the deliverance of data in order to meet the high bandwidth and low latency of SDN strict QoS specifications. This requires two modules. Since graphical systems are called stupid and all the knowledge on the control centres is preserved. In addition to providing quick and efficient communication, embedding SDN in multimedia studies can contribute to convenient power.

Min [23] suggest a multi-modal network topic model (CM3TM) able to: 1) distinguish between two various kind of topics; i.e, only platform-specific topics that are important for a given platform; 2) align various modalities from different platforms and exchange information. In particular, CM3TM not only can separate and concurrently learn the space into the general theme and platform-specific themes, but also allows for alignment with the various methods through the learned subject field. CM3TM may differentiate between popular topics and platform relevant subjects and coordinate subjects across channels on various modalities. CM3TM is very robust and can be applied in social multimedia analysis to other cross-platform suggestion topics. The assessment shows its efficacy in linking diverse channels to multiple modalities via our customised interplatform suggestion applications added location-context.

3. Proposed System:

The main purpose of this project is to create safe contact between the sender and the recipient through emails and other modes of communication. The proposed study covers the scope methodology for integration of data into IWT coefficients of high frequencies. In this paper a modern lossless hiding approach is introduced for digital images utilising the transformation of integral wavelets and the threshold embedding. The suggested method first decomposes the input picture with the transformation of the integer wavelet (IWT). In order to conceal confidential knowledge the sub-bands frequency (LL, HH, HL, and LH) are prepared. The adjustments are rendered such that the proposed solution is essentially shielded from results. When data are inserted into such high-frequency IWT coefficients, the wavelet may transform to remove data from images after the reverse integer. Photos have been a repository of knowledge that is unavoidable. If photographs are private and we want a reliable and protected delivery of the file, encryption is at work. The methodology used in this paper is cryptography of the Elliptic Curve (ECC). You may encrypt your stegno picture with ECC Encryption. Different ECC experiments also concluded that the elliptic curve cryptography challenging to
overcome is exponentially difficult with regard to the key size used. This makes ECC an outstanding alternative for encryption/decryption relative to other methods in cryptography that are linearly complicated or sub-exponentially difficult. Use the hiding key to retrieve the hidden data and to restore the picture using the decryption key. The receiver will Figure 1 defines the proposed framework.

![Proposed System Architecture](image)

**Figure 1.** Proposed System Architecture.

3.1. Data Preprocessing

Data hiding is the hidden message hiding method in the cover file. To exchange details, sender and receiver should log. The detail of the registration is saved in the database and the password is exclusive. Secret message in text format is present and the picture cover file is chosen. In order to build a steganographic, the submitted text message was secret. Generate the key to safely exchange the recipient information. To exchange details, pick the recipient name.

3.2. Integer Wavelet Transformation

The cover picture is first decomposed with IWT in the data hiding process. Then high frequency (LH, HL, HH) coefficients are pre-processed to integrate hidden details. Picture 2 histogram is observed and two meaning levels (T1, T2) are selected. To mask the bits in the frame. This figure will be obtained by counting the availability of the exact number of the specified threshold levels. The purpose of this suggested approach is to minimise the centred peak of the histogram, and to transfer values to both sides of the selected threshold level and thereby to hidden results. If the embedding bit is 1 then the i2 coefficients will be added by 1, if the embedding bit is 0 the i2 coefficients stay the same. In comparison, the i2 coefficients will be added by 1 to this. This method proceeds until the message pieces are ended. The histogram top is transferred on both sides of the threshold values, which results in the initial picture details being obscured.

3.3. Image Encryption

Cryptography is a method of data storage and conversion through an accurate procedure in order that it can be recited and processed by only individuals to whom it is expected. Cryptography requires such methods as microdotal, fusion of images and alternate ways to store and transmit fleece content. The picture representing the content may be encoded on a public key basis. The ECC encryption method maps a pixel value from the input picture to an Elliptical curve position. If the next time the same valued pixel is seen, an adjacent column object is mapped into the same row. rehashes from the primary segment of the planning table every pixel esteem in the wake of planning (T-1) segment
focuses. After all pixel values are mapped in the plain picture, the mapped points are encrypted using the recipient's public key. In two dots, the encryption of a planned point results, one point is similar to all pixels, while the other point is distinct. In Elliptic curve the constants a and b are described. The cyclic subgroup is then described by its point G. The public key encryption is also known. The \( y^2 = x^3 + ax + b \) is the equation of an elliptical curve. Key public and private key generation is highly critical. The transmitter encrypts the message with a client with a public key and is decrypted per user. Public key \( Q = dp \) is used while the chosen random number for the range from 1 to \( n-1 \) is \( d = \text{random number} \). The public key \( d \) is a private key, \( P = \text{dot on curve Q} \). For future purposes, the encrypted picture can be used.

3.4. Image Decryption

The recipient will decode the initial picture to be exchanged by the sender. The recipient uses its private key to decode the picture of the chip when decrypting the chipboard. Authenticity offers evidence that the letter has been delivered to the correct sender and that the message has not been altered or modified during transit.

3.5. Data Extraction

The extraction of data is the initial data extraction method. The receiver receives the hidden cover picture post. During the message sending method, a special key is created and exchanged with the recipient. On the recipient's hand, an encoded hidden message may be correctly retrieved using the data cover key. By converting the reverse wavelet, all frequency components (LL), (LH), (HL) may be integrated (HH). The user will retrieve the picture after integrating frequency components. You will perfectly retrieve the original picture with the hiding key and decryption key.

4. Results and Discussion

The suggested system was enforced with the help of Intel processor 2.6.0 GHZ and 2GB RAM. The proposed Front End has been out with the help of ASP.NET. The Back End of the proposed system was carried with the help of SQL SERVER. We hold chosen six regular dark-scale images1 from our experiment, which appears in Fig.2. As cover photographs, each having a size of 512 per day, Lena, F16, Sail, Peppers, Baboon and Lake are used as covers. The visual consistency of the obtained picture in PSNR (dB) and in bits per pixel (bpp) for determining the output of the proposed method is used. The PSNR is formulated as

\[
\text{PSNR} = 20 \log_{10} \left( \frac{\text{Max}(X(i,j))}{\sqrt{MSE}} \right)
\]

\[
MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j) - X^w(i,j))^2
\]

The measurements of the original picture are \( M \) and \( N \) in this comparison, and MSE is the median square error between \( X \) and \( X^w \) diametrical. If the PSNR is strong, it indicates that the host picture is less influenced by the integration phase and more invisible.
Figure 2. Six Standard Test Images.

The proposed execution screen shots are defined in the 3 to 11. e. Table 1 provides two forms of inserting rate, firstly the overall inserting rate (including the additional details and the LSB of boundary pixels) (which involves just additional data). Due to high amounts of terrible white pixels, the pure Baboon incorporation rate is lower than that in other images. In other photos, pure integration rate is near the full integration rate, which indicates that terrible white pixels do not impact the built-in power. In addition, the confidential key for Paillier cryptosystem is straightforwardly used for decrypting the marked encrypted picture. Table 1 displays the PSNR for the six pictures (Fig. 4) of the filtered and restored picture that are explicitly decrypted in the medium. We will examine that the filtered image PSNR in Table 1, which is explicitly decrypted, is greatly enhanced over the PSNR, and the restored image is retrieved by the process suggested without lossing. In accordance with the Paillier cryptosystem's homomorphic property, encryption leads to the expansion of the pixel value, particularly using long public encryption keys. We took account of $N = 17$ to 19 in our experiment, which shifts the coded pixels from 8 bits to 17 bits, to reveal all phases of our proposed models. Please notice that changing the pixel range would just contribute to the data units for each pixel being extended. Indeed the pixel count remains identical to the initial pixel count.
Table 1. Execution investigation of proposed technique.

| Picture | No. of terrible white pixels | PSNR (dB) | Implanting rate (bpp) |
|---------|-----------------------------|----------|----------------------|
|         | Precisely | Refined | Recreated | Absolute | Authentic |
| Lena    | 0         | 12.056  | 29.337    | +∞       | 0.4833     | 0.4833     |
| F16     | 2         | 12.043  | 27.297    | +∞       | 0.4833     | 0.4829     |
| Boat    | 28        | 12.037  | 26.989    | +∞       | 0.4832     | 0.4816     |
| Peppers | 3         | 12.037  | 28.744    | +∞       | 0.4833     | 0.4820     |
| Baboon  | 294       | 12.042  | 21.299    | +∞       | 0.4832     | 0.4641     |
| Lake    | 1         | 12.045  | 26.142    | +∞       | 0.4833     | 0.4832     |

5. Conclusion
This paper proposes a reversible data hiding technique based on the integer wavelet transform technique. The data hiding capacity and speed is increased by combining IWT with ECC Encryption. After embedding data onto the image region, both original and stego image are similar to each other. For data hiding, the transformation domain is used. This main knowledge is integrated by preprocessing and bit exchange in the higher frequency coefficients of integer wavelet transformation. The photo will then be secured using the ECC Encryption. Encryption helps boost communication domain protection. The fantastic combined unit energy that is the incredibly scalable design of both strategies often offers the capacity to further build and enhance the freedom of these geospatial activities by adding brand-new computation phases much like the sum of error corrections.

6. References:
[1] Tian H, Zhao Y, Ni R, Qin L, Li X 2013 Ldft-based watermarking resilient to local desynchronization attacks 43(6) IEEE Trans Cybern 2190–201.
[2] Tian J 2003 Reversible data embedding using a difference expansion 13(8) IEEE Trans Circuits Syst Video Technol 890–6.
[3] Ni Z, Shi Y-Q, Ansari N, Su W 2006 Reversible data hiding 16(3) IEEE Trans Circuits Syst Video Technol 354–62.
[4] Fridrich J, Goljan M, Du R 2001 Invertible authentication. In: Security and watermarking of multimedia contents III International Society for Optics and Photonics 197–209.
[5] Sachnev V, Kim HJ, Nam J, Suresh S, Shi YQ 2009 Reversible watermarking algorithm using sorting and prediction 19(7) IEEE Trans Circuits Syst Video Technol 989–99.
[6] Malik A, Wang H, Wu H, Abdullahi SM 2019 Reversible data hiding with multiple data for multiple users in an encrypted image 11(1) International J Digit Crime Forensics (IJDCF) 46–61.