Novel Approach for Preserving Intellectual Property Rights For Image Using DWT and Data Mining ID3 algorithm

Falguni Tank¹, Prof. Daxa Vekariya²

¹PG Student, Department of Computer Engineering, Noble Group of Institutions, Junagadh, India
²Assistant Professor, Department of Computer Engineering, Noble Group of Institutions, Junagadh, India

Abstract — Security of data is a challenging issue and transmitting the Secured data is again most challenging. Data hiding from intruders and also hiding the fact that any data is hidden is one of the techniques to hide the data in a secured way called Steganography. In this proposed system secret image is hidden behind the image using DWT and ID3 algorithm. DWT Decompose the image into 4-high and low frequency sub-bands. ID3 algorithm is used to select the proper pixel to hide the image. Here we have also used RSA algorithm for applying security on secret image. Thus, this is a Secured manner to hide the image on image.

Keywords- Steganography, Decision tree, DWT, RSA, Arnold transform, weka.

I. INTRODUCTION

The word steganography comes from the Greek steganos, meaning covered or secret, and graphy, meaning writing or drawing. Therefore, “Reference [1] steganography literally means covered writing. Steganography simply takes one piece of information and hides it within another.”

“Stego-medium = Cover medium + Secret message + Stego key “.

DWT-based watermarking techniques, the DWT coefficients are modified to watermark data. Divides the image into 4 parts LL, HL, LH, and HH. The LL part is a down sampled and low resolution version of the Cover image. “Reference [2] Discrete wavelet transform (DWT), which transforms a discrete time signal to a discrete wavelet representation. it converts an input series x₀, x₁, ... xₙ into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series”. “Reference [3] propose all process in image on LL Bend(Alpha Bend) and represents the approximate version of the original at half the resolution.” Also give more smoothing effect & smooth regions.

“Reference [10] we apply all process in image on LL Bend(Alpha Bend) and represents the approximate version of the original at half the resolution.” Also give more smoothing effect & smooth regions.

“Reference [11] This proposed system give Copyright protection through Arnold transform and RSA.” “Reference [6] For hiding data we can use here Generate Decision Tree that give the proper pixels for embedding secret image on cover image using this data mining ID3.”

“Reference [3] proposed a steganography technique for hiding multiple images based on DWT and DCT.” “Reference [4] proposed a modified high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image.” “Reference [5] proposed a Scrambling transformation is usually applied in the pretreatment stage of watermarking as a means of encrypted technology.”

“Reference [7] proposed Performance Analysis of Image Steganography based on DWT and Arnold Transform.” “Reference [8] PSNR values of the Arnold Transform based method are better than existing methods. for security purpose RSA can be used “. RSA is consider as a strong asymmetric key cryptographic technique. “Reference [9] proposed combined version of Arnold’s transformation and RSA algorithm for the watermark encryption.” For the robustness, DWT has been taken for the domain transformation.

In this paper purposes a steganography techniques based on DWT with Arnold transform & Selective proper pixels using decision tree for embedding the secret image & producing high fidelity stego image. We improve Our purposed technique so we use RSA technique for security & against Attacks.

II. DISCRETE WAVELET TRANSFORM (DWT)

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. Where, L represents low-pass filter, H represents high-pass filter. The information of low frequency district is a image close to the original image. . Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.so, we apply all process of steganography on Alpha blend(LL).
III. ID3 ALGORITHM

ID3, Iterative Dichotomiser 3 is a decision tree learning algorithm which is used for the classification of the objects with the iterative inductive approach. In this algorithm the top to down approach is used. The top node is called as the root node and others are the leaf nodes. So it’s a traversing from root node to leaf nodes. Each node requires some test on the attributes which decide the level of the leaf nodes. These decision trees are mostly used for the decision making purpose.

The decision tree learning algorithms are mainly used because of the three reasons:
1. Decision tree is a good infer from the particular cases that are unobserved instance.
2. The calculations in these methods are efficient and are proportional to the instances that are observed.
3. At the final, the decision tree which is produced is easily understood by the human.

IV. ARNOLD TRANSFORM

An image transformation is done to randomize the actual pixel positions of the image. After several iterations the actual image reappears. The number of iterations taken to change the pixel positions is defined as Arnold’s period. The periods change in correspondence to the size of images i.e. when the size of the image increases, Arnold’s period also increases. The Arnold’s transformation is represented as:

\[
\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod n
\]

Where, variable \( n \) denotes image size. Equation (1) represents Arnold’s transformation which is used to change all pixel coordinates of the image being taken. After all the coordinates have been transformed, we got a scrambled image. After several fixed number of iterations, the scrambled image is formed. The decryption process depends on period of transformation.

V. RSA FOR SECURITY

RSA Algorithm [11], named after its developers (Ranald Rivest, Adi Shamir, and Leonard Adleman) uses variable size encryption blocks and variable size keys. Being a method of public key cryptography, it involves two keys, viz. a private key and a public key. The key-pairs are derived from a large integer which is the product of two prime numbers chosen as per some special rule and create an RSA public/private key pair.

VI. PROPOSED SYSTEM

In this section, We are using DWT for hiding stego data in cover image. For higher security used Arnold transform & image can be scrambled. and after embed stego image into original image.

A. Steps of Overview of proposed System as follows:

Step1: First take cover image and secret image.
Step2: Embedded Secret image in the cover image using watermark technique.
Step3: Then Apply Key Generation RSA on Watermarking image and secure with Secret key.
Step 4: Get Stego image.
Step5: Extract Key from Stego image for Extract Secret image.
Step 6: Apply key on the Stego image and Get Secret image.

The fig. 2 shows Overview of proposed system.

B. Steps of embedding process of proposed System as follows:

Step 1: First take original image (Cover image) and Secret image.
Step 2: DWT on the both image & Get LL bend is use for embedded data.
Step 3: Apply ID3 Algorithm using Weka tool on cover image and other side apply Arnold transform on secret image.
Step 4: After get Decision tree to give proper pixels for embedding scrambled image on cover image.
Step 5: Apply IDWT (Inverse Discrete Wavelet transform) to get watermark image.
C. **Steps of Stego Image Generation as follows:**

Step1: First select Area for insert stego key in watermarking image.
Step2: Identify x & y co-ordinate to insert stego key.
Step3: Key Generate using RSA Algorithm and put key in the selected Area.
Step4: Then store key location (x, y) on boundary of image.
Step5: After get Stego image.

![Diagram of Stego Image Generation](image)

**Fig3.** Embedding process in Steganography

D. **Steps of Secret image extraction of proposed System as follows:**

Step1: First read Boundary pixel for get location of secret key.
Step2: Then get secret key from location (x, y).
Step3: Apply Secret key on image and extract secret image.
E. Steps of Extraction process as follows:

Step1: first apply DWT on Watermark image.
Step2: Then extract cover image and scrambled image.
Step3: After apply Arnold transform on Scrambled image.
Step4: Then apply IDWT on both images.
Step5: Get original image and Secret image.

VII. OBJECTIVE ANALYSIS AND ATTACK ANALYSIS
A. Objective Analysis

The phrase **peak signal-to-noise ratio**, often abbreviated **PSNR**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

It is most easily defined via the mean squared error (**MSE**) which for two \(m\times n\) monochrome images \(I\) and \(K\) where one of the images is considered a noisy approximation of the other is defined as:

\[
\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2
\]

The PSNR is defined as:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{NAX^2}{\text{MSE}} \right)
\]

B. Attack Analysis

The proposed Scheme of the System can Withstand various attacks like compression Attack, destroy Everything attack, visual attack, statical attack. The RSA Algorithm that is used for security can recover attacks like brute force, timing attacks, chosen cipher text text attacks.

VIII. CONCLUSIONS

The proposed system help to transmit and receive the secret image in a highly secured manner by using DWT & Arnold transform. The System is robust against the possible attacks on the system. Hence, it can serve as better & effective way to maintain the security of the image.

REFERENCES