DIGITAL IMAGE WATERMARKING FOR IMAGE PROTECTION

Ms. P. DEVI, ASSISTANT PROFESSOR (Sr.Gr.)
Department of Electronics and Communication Engineering
Sri Ramakrishna Institute of Technology, Coimbatore-10

SIBICHAKRAVARATHY NI
Department of Electronics and Communication Engineering
Sri Ramakrishna Institute of Technology, Coimbatore-10

UDHAYAPRAKASH A
Department of Electronics and Communication Engineering
Sri Ramakrishna Institute of Technology, Coimbatore-10

YAVINRAJ S
Department of Electronics and Communication Engineering
Sri Ramakrishna Institute of Technology, Coimbatore-10

YOGESHKUMAR S
Department of Electronics and Communication Engineering
Sri Ramakrishna Institute of Technology, Coimbatore-10

ABSTRACT--For the purpose of copyright security for sight and sound information, computerized watermarking innovation has drawn in increasingly more consideration in different exploration fields. Analysts have started to investigate the achievability of applying it to include picture detecting information as of late. On account of the distinction of remote detecting picture, higher prerequisites are advanced for its security and the board, particularly for the copyright assurance, illicit use and credibility ID of remote detecting picture information. Accordingly, this paper proposes to utilize picture watermarking innovation to accomplish complete security insurance of remote detecting picture information, while the utilization of cryptography innovation expands the appropriateness and security of watermarking innovation. The exploratory outcomes show that the plan of remote detecting picture advanced watermarking innovation has great execution in the indistinctness and vigor of watermarking.

Keywords – Watermarking, Mallat Wavelet, DWT, PSNR

I. INTRODUCTION

Computerized watermarking is the most common way of passing on data by indistinctly inserting it into the advanced media. The reason for installing such data relies upon the application and the requirements of the proprietor/client of the advanced media. Ebb and flow fundamental uses of watermarking incorporate the accompanying:
1. Copyright insurance: The goal is to install data about the source/proprietor of the advanced media to keep different gatherings from asserting the responsibility for media.
2. Fingerprinting: The target of fingerprinting is to pass on data about the beneficiary of the computerized media (rather than the
3. Duplicate security: Watermarking can be utilized to control information replicating gadgets and keep them from duplicating the advanced media on the off chance that the watermark implanted in the media demonstrates that media is duplicate ensured.

4. Picture validation: The goal is to really take a look at the legitimacy of the advanced media. This requires the location of adjustments to the information. This venture doesn't explicitly zero in on a solitary utilization of watermarking. Rather, it implements several different watermarking algorithms which may or may not be desirable for a variety of applications. However, I only focus on watermarking of images.

II. PROPOSED ALGORITHM

2.1 SECURITY ENCRYPTION:

Scrambling transformation is a widely used method in digital image encryption. Image scrambling technology makes use of the characteristics of digital image with digital matrix to scramble the position or colour of the pixels in the image and turn it into a disorderly image in order to achieve the effect of confidentiality. In Arnold Cat transform algorithm is used to scramble the image. This algorithm has good scrambling effect and simple operation. Arnold scrambling is used in this paper. Arnold scrambling can noise the watermarking, make the energy of the image as uniform as possible, effectively improve the security and robustness of the hidden information, and can use its periodicity to reverse transform and restore the image scrambling.

Arnold transformation is defined as follows:

For any \( N \times N \) matrix, let \( x \) and \( y \) be the original subscripts of matrix elements. After Arnold transformation, the new subscripts are \( x' \) and \( y' \), and the following formula is:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 11 \\ 12 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \tag{1}
\]

\( x, y = 0, 1, \ldots, N-1 \)

Note formula 1 as transform matrix \( A \), the \((x, y)^T\) is input, \((x', y')^T\) is output. Considering its feedback, the following iterations can be made:

\[
P_{xy}^{n+1} = A_{xy}^n (mod N) \tag{2}
\]

\[
P_{xy}^n = (x, y)^T
\]

Where \( n \) indicates iteration times. Image information (such as gray level) is transplanted with replacement of discrete matrix. When all points in the original image are traversed, a new image is generated.

2.2 WAVELET TRANSFORM:

The idea of wavelet transform and the selection of embedding frequency band make use of Mallat tower decomposition algorithm. The image is decomposed into detail coefficients \( LH_n, HL_n, HH_n \) and approximation coefficients \( LL_n \) on \( N \) scales, and \( N=1,2,\ldots, N \). \( LL \) are the details obtained after filtering in the lowest frequency band. \( HH \) retains the detail information after filtering in both horizontal and vertical directions. The decomposition formulas of the Mallat algorithm for discrete sequences are as follows:

\[
A_{j+1}(n) = H(n) \times A_j (n) = \sum_k H(k)A_j (2n-k). \tag{3}
\]

\[
D_{j+1}(n) = G(n) \times A_j (n) = \sum_k G(k)A_j (2n-k). \tag{4}
\]

Where \( H(n) \) and \( G(n) \) represent tap coefficients of low-pass and high-pass filters corresponding to the selected wavelet functions respectively. The reconstruction formulas of the Mallat algorithm for discrete sequences are as follows:

\[
A_j(n) = h(n) \times A_{j+1} (n) + g(n) \times D_{j+1} (n)
= \sum_k h(n-2k) A_{j+1}(k)
+ \sum_k g(n-2k) D_{j+1}(k) \tag{5}
\]
Where $h(n)$ and $g(n)$ represent the same coefficients with $H(n)$ and $G(n)$. The two-dimensional image DWT transform decomposition

![DWT Decomposition model](image)

### Figure 1. DWT Decomposition model

#### 2.3 THE PROPOSED DIGITAL WATERMARKING IMAGE:

The basic frame of watermark embedding procedure is as follows in figure 2. This watermark algorithm introduces a series of enhancement mechanisms, such as. In addition, the watermark algorithm supports both robust watermark and semi-fragile watermark, which makes the watermarking scheme, can have functions such as copyright protection and content integrity verification.

![Masking characteristic of image](image)

(a) Lena Image  
(b) Visual masking

Fig 2 Masking characteristic of image
2.4 BLOCK DIAGRAM OF WATERMARK ALGORITHM PROCEDURE:

3. RESULT:

In this scheme, we design a remote sensing image security protection scheme based on digital watermarking. The scheme realizes robust watermarking and semi-fragile watermarking by means of block image DWT transform and coefficient quantization. Robust watermark is constructed from binary image and semi-fragile watermark is constructed from pseudo-random sequence. In order to verify the performance of this algorithm, the following experiments are simulated. The simulation experiments are mainly carried out in two aspects:

(1) verifying the invisibility of watermark,
(2) verifying the robustness of watermark.
4. REFERENCES


