International Journal of scientific research and management (IJSRM)
||Volume||2||Issue||10||Pages||1494-1497||2014||
Website: www.ijsrm.in ISSN (e): 2321-3418

An Efficient Encrypted Digital Image Watermarking Scheme

[1]Kavitha Kapala, [2]Jagadeeswararao G

[1] Aditya Institute of Technology And Management, Tekkali, India
Kavitha.akki@gmail.com

[2]Aditya Institute of Technology And Management, Tekkali, India
eshwar.mtech@gmail.com

Abstract: Increasing in networked multimedia systems has an immediate need for copyright protection and security of multimedia data that is transferred through the network. Digital watermarking technology provides solutions for protecting multimedia data from illegal manipulations. In the proposed method, embedding of watermark is done by using Discrete Wavelet Transform (DWT) - Singular Value Decomposition (SVD), and then a private key is used for the encryption of watermarked image. At the other end the watermarked image is decrypted first using the private key then the watermark is extracted by applying the reverse process of embedding. Using DWT-SVD, modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks, and without having the private key any one cannot delete or modify the watermark.

Keywords: Watermarking, Color image, Block division, Invisible watermarking.

1. Introduction

With the vast usage and development of digitized technology, computer science, communication and network, image data transformation services are widely implemented and applied. Also, there are many new challenges in image data information industry, such as pirate, juggle and spread abroad. So many people concerned about image encryption. An effective way to solve these problems in this field is using Digital Watermarking [1].Watermark is an invisible signature embedded inside an image to show authenticity or proof of ownership.

Depending on the type of information needed by the detector, watermarking schemes are classified into 3 types:

- Non-blind schemes: Both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes: The secret key(s) and the watermark bit sequence.
- Blind schemes: Only the secret key(s) [6].

A watermarking process consists of the watermark, an embedding algorithm, and an extraction, or detection, algorithm. Watermarks can be embedded in the spatial domain or a transform domain. The major advantage of transform domain methods is their superior robustness to common image distortions. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity [3].

2. Digital Image Watermarking Using Dwt-Svd:

2.1 Digital Watermarking Techniques:

Watermarking takes place either in the spatial domain, where the addition of the watermark is done directly to the pixel values of the image, or in a transformed domain like discrete cosine transformed domain (DCT) or the discrete wavelet transformed domain (DWT). The watermarking in a transformed domain provides more robustness to many forms of attack. The basic requirement of a watermarking scheme is a watermark embedding system and a watermark extraction system. The input to a watermark embedding system is either a randomly generated sequence of bits or the watermark itself and the output is the watermarked image. The watermark extraction system is used to determine whether or not a watermark has been added.

2.2 Haar Discrete Wavelet Transform:

The Haar wavelet transform is one kind of wavelet transform. A digital image *I* with m x n pixels is transformed to the DWT frequency domain as follows. First, an original image can be decomposed into a low frequency band LL1 and three high frequency bands LH1, HL1 and HH1. Applying the DWT on the low frequency band LL1 again will generate four lower-resolution sub-bands LL2, LH2, HL2 and HH2. This process is continued an arbitrary number of times, which is usually determined by the application at hand. The approximate image band LL holds the most important information of the original image. The LH, HL and HH bands contain some high-frequency information about the edge components of the signal. Furthermore, from these DWT coefficients; the original signal can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). An image can be decomposed into a pyramid structure as shown below. Figure (a).shows the image “Lena” and the transformed result after the two-level DWT transformation.

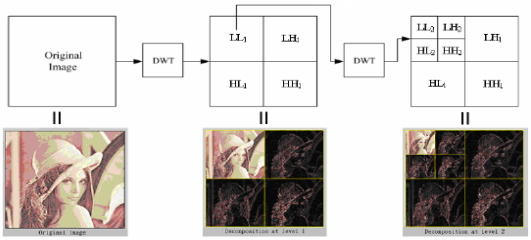


Figure (a): Two-level DWT transformation of color image "Lena"

$LL_1(x,y) = 1/4 \sum_{i=0}^{1}\sum_{j=0}^{1} I(2x+i, 2y+j)$ (2.1)

$LH_1(x,y) = 1/4 \sum_{i=0}^{1} I(2x+i, 2y) - 1/4\sum_{i=0}^{1} I(2x+i, 2y+1)$ (2.2)

$HL_1(x,y) = 1/4 \sum_{j=0}^{1} I(2x, 2y+j) - 1/4 \sum_{j=0}^{1} I(2x+1, 2y+j)$ (2.3)

$HH_1(x,y) = 1/4$ {I(2x,2y)+I(2x+1,2y+1)- I(2x+1,2y)-I(2x,2y+1)} (2.4)

The above equations generate the components of LL_1, LH_1, HL_1 and HH_1 respectively.
$(0 \le x \le \frac{m}{2}, 0 \le x \le \frac{n}{2})$, where (x,y) denote the pixel location in the host image.

In this scheme, the thirteen subbands after the three-level DWT on the color host image are shown in Figure (b). The middle frequency subbands after the three-level DWT, denoted as 1^n (n=1,2,3 and 4) are used for watermark embedding.

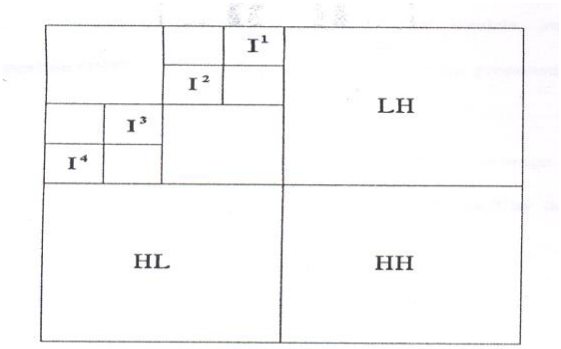


Figure (b): The sub bands after the three-level DWT in the proposed scheme

2.3 Singular Value Decomposition:

Singular Value Decomposition (SVD) is a mathematical tool used to analyze matrices. SVD is a widely used technique to decompose a matrix into several component matrices, exposing many of the useful and interesting properties of the original matrix. The decomposition of a matrix is often called a 'factorization'. Ideally, the matrix is decomposed into a set of factors (often orthogonal or independent) that are optimal based on some criterion. For example, a criterion might be the reconstruction of the decomposed matrix. The SVD, in general, represents an expansion of the original data in a coordinate system where the covariance matrix is diagonal. The eigen matrix in the singular value decomposition is explored for data embedding.

Any real mxn matrix A can be decomposed uniquely as

$A = UDV^{T.}$

Here U and V are orthogonal, and D is a square diagonal. That is $UU^T = I_{rank\ (A)}$, and $VV^T = I_{rank\ (A)}$, where U is rank (A) x m, V is rank (A) x n.

D is rank (A) x rank (A) diagonal matrix given by,

$D = diag\ (\sigma_1, \sigma_2 \ldots \sigma_{rank\ (A)})$ ordered so that $\sigma_1 \ge \sigma_2 \ge \ldots \ge \sigma_{rank\ (A)} > 0$, are the singular values of A, or the square roots of the eigen values of AA^T and A^TA. Each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer.

If $U = (u_1, u_2, \ldots, u_n)$ and $V = (v_1, v_2, \ldots, v_n)$, then,

$A = \sum_{i=1}^{r} \sigma\, u_i v_i^T$. (Where r is the rank of matrix A).

2.4 Cryptography

Cryptography techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. Only the use of a secret key can convert the cipher text back into human readable (clear text) form. In the proposed method symmetric encryption technique is used. This type of cryptography technique uses just a single key. The sender applies a private key to encrypt the watermarked image and then transferred through the network, at the receiver side the encrypted watermarked image is decrypted using the same private key and then the watermark is extracted by the receiver.

2.5 Attacks

If a file is generated containing a watermark for copyright reasons, some other party may wish to use it without paying royalties to the owner. Instead, they use techniques known as attacks on the watermark to either remove it or make it difficult to uniquely identify the owner. It is possible to attack the file in transport between client and copyright authority. Many types of attacks are used and an algorithm for embedding the watermark should be robust against all attacks without affecting the quality of the image.

The robustness of watermarked image is calculated by using Normalized Cross-Correlation defined as

$$NC = \frac{\sum_i \sum_j \left(x_{ij} - \bar{x}\right)\left(x_{ij}' - \bar{x}'\right)}{\sqrt{\left[\sum_i \sum_j \left(x_{ij} - \bar{x}\right)^2\right]\left[\sum_i \sum_j \left(x_{ij}' - \bar{x}'\right)^2\right]}}$$

Watermark image is denoted by x_{ij}, and the extracted watermark is denoted by x_{ij}'.

$\bar{x}$, and $\bar{x}'$ indicate the mean of the original watermark and extracted watermark respectively.

3. Watermarking Process

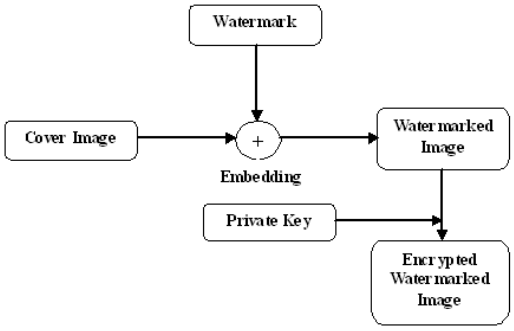
3.1 Watermark Embedding Algorithm

1. Read the cover image (A).
2. Using DWT decompose the cover image into 4 sub bands : LL,HL,LH and HH.
3. Apply SVD to each sub band of encrypted image
   $A_i = U_i S_i V_i^T$, i=1,2,3,4
   where i denotes LL, HL, LH and HH sub bands.
4. Apply SVD to the watermark.
   $W = U_w S_w V_w^T$. where W= watermark.
5. Modify the singular values of cover image by embedding singular values of W, such that

   $S^*_i = S_i + \alpha S_w$, i=1,2,3,4

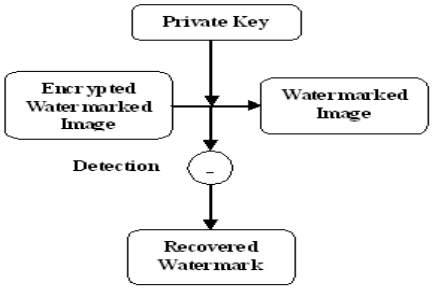
where S^*_i is modified singular matrix of A_i, α is the scaling factor used to control the strength of watermark signal.

6. Obtain the four sets of modified DWT coefficients of image. $A^*_i=U^*_iS^*_iV^{*T}_i$.
7. Apply the inverse DWT to the four sets of modified DWT coefficients to produce the watermarked image.
8. The watermarked image is encrypted with a private K_D , now obtain the encrypted watermarked image.



3.2 Watermark Extraction Algorithm

1. Decrypt the encrypted watermarked image with private key (K_D) to get the decrypted watermarked image(A^*).
2. Using DWT decompose the image A^* into 4 sub bands: LL,HL,LH and HH.
3. Apply SVD to each sub band of image $A^*_i= U^*_iS^*_iV^{*T}_i$, i=1,2,3,4 where i denotes LL, HL, LH and HH sub bands.
4. Extract the singular values from each sub band and construct the watermarks using singular vectors: $W_i=U_{wi}S_{wi}V_{wi}^T$, i=1,2,3,4 where i denotes LL, HL, LH and HH sub bands.



4. Results

Figure 4.1 Cover Image

Figure 4.2 Watermark Image

Figure4.3Watermarkedimage

Figure 4.4 Retrieved Watermarks.

Figure4.1, 4.2, 4.3, 4.4 shows the 512x512 gray scale cover image Lena, the 256X256 gray scale visual watermark AITAM logo, the watermarked cover image, and the visual watermarks constructed from the four quadrants.

a) Watermarked Image subjected to median filtering attack

Retrieved Watermarks with NC values:

b)Watermarked Image subjected to Histogram equalization attack :

Retrieved Watermarks with NC values:

c) Watermarked Image subjected to rotation (10^0) attack

Retrieved Watermarks with NC values:

d) Watermarked Image subjected to Average Filtering 3 x 3 mask attack

Retrieved Watermarks with NC values:

e) Watermarked Image subjected to salt & pepper 0.01 attack

Retrieved Watermarks with NC values:

Table 1 : Obtained NC Values

Type of Attack	*NC Value*			
	LL	*LH*	*HL*	*HH*
median filtering attack	0.6827	0.8027	0.9174	0.8527
Histogram equalization	0.9356	0.8227	0.8146	0.8227
rotation (10^0)	0.6772	0.7960	0.8971	0.8527
Average Filtering 3 x 3 mask	0.7569	0.7637	0.8438	0.8399
salt & pepper 0.01	0.6836	0.7743	0.7559	0.7721

5. Conclusions

The scaling factor can be chosen from a fairly wide range of values for LL1, and also for the other three quadrants. As quadrant LL1 contains the largest DWT coefficients, the scaling factor is chosen accordingly. Watermarks inserted in the lowest frequencies (LL1) are resistant to one group of attacks, and watermarks embedded in highest frequencies (HH1) are resistant to another group of attacks. A comparison of the hybrid DWT-SVD watermarking scheme with a pure SVD based algorithm shows that the proposed scheme performs much better, providing more robustness and reliability.

References:

[1] Ms. Roshan Jahan ,GBTU ,Lucknow, India "Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption" *International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 10, October 2013 ISSN: 2278 – 7798*

[2] Preeti Gupta, " Cryptography based digital image watermarking algorithm to increase security of watermark data "International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 1 ISSN 2229-5518

[3] Praful Saxena, Shanon Garg and Arpita Srivastava "DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band" 2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April 28-29, 2012.

[4] Ms. Roshan Jahan ,GBTU ,Lucknow, India "Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption" *International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 10, October 2013 ISSN: 2278 – 7798*

[5] Keiichi Kuroda, Masakatsu Nishigaki, Masakazu Soga, Akio Takubo, and Itsukazu Nakamura A Digital Watermark using Public-key Cryptography for Open Algorithm ICITA2002 ISBN: 1-86467-114-9

[6] Emir Ganic, Ahmet M. Eskicioglu Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies.

[7] Baisa L. Gunjal and Suresh N.Mali, "secured color image watermarking technique in dwt-dct domain "International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, August 2011

Author Profile

Kavitha Kapala received her M.Tech (CSE) from JNTUK. Presently she is working as a Sr. Assistant Professor in the department of Information Technology, AITAM, Tekkali Andhra Pradesh, India. Her areas of interest include Information Security and Image Processing.