Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Encryption of Watermarked Images using Chakra Symmetric Key Approach

Sk.Shamshad[#1], K.L.Sailaja[*2], P.Rameshkumar[#3]
Department of Computer Science and Engineering
V.R.Siddhartha Engineering College
Vijayawada, Andhra Pradesh, India

Abstract—Watermarking is the process of embedding new data into image, audio or video. Digital Watermarking technique is used to hide a secret or personal message to protect a products copyright or to demonstrate data integrity. To provide double protection, after the watermarking process, the watermarked image tends to go through an encryption process using CHAKRA – symmetry key encryption algorithm which encrypts the data with the concepts of Cartesian coordinate geometry and circle generation. In this paper, we perform watermarking on different types of images like BMP, JPEG etc.., and the input image is pre-processed and converted into JPEG-LS format which contains enhanced quality.

Keywords—JPEG-LS Image, Watermarking, Chakra Symmetric Key Encryption, Decryption, Watermark Detection.

I. INTRODUCTION

Digital Watermarking technique is used to hide a small amount of digital data in a digital signal in such a way that it can't be detected by viewer. A digital watermark can be either visible or invisible.

A *visible* watermark is a visible semi-transparent text or image overlaid on the original image. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner's property. *Visible* watermarks are more robust against image transformation especially if we use a semi-transparent watermark placed over whole image[9]. Thus they are preferable for strong copyright protection of intellectual property that's in digital format.

An *invisible* watermark is an embedded image which cannot be perceived with human's eyes. Only electronic devices or specialized software can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content like text, images or even audio content to prove its authenticity[9]. Typical applications of digital watermarking can include broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control legacy enhancement and content description.

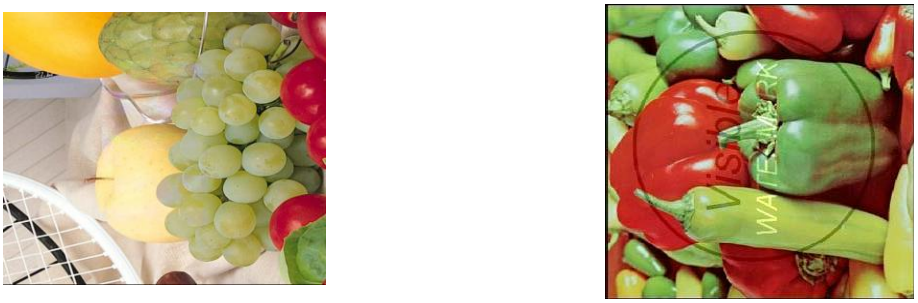


Figure1:Visible and Invisible Watermarked Images

II DIFFERENT DOMAINS IN WATERMARKING TECHNIQUES

The digital image watermarking techniques in the literature are typically grouped in two classes: Spatial domain techniques [5]: which embed the watermark by modifying the pixel values of the original image and the transform domain techniques which embed the watermark in the domain of an invertible transform. The discrete cosines transform (DCT) and the discrete wavelet transform (DWT) are commonly used for watermarking purposes[6].

The transform domain algorithms modify a subset of the transform coefficients with the watermarking data and generally achieve better robustness than spatial domain methods.

A. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It converts a spatial domain waveform into its constituent frequency components as represented by a set of coefficients. The process of reconstructing a set of spatial domain samples is called the Inverse Discrete Cosine Transform (IDCT). It is widely used in image compression.

B. Discrete Wavelet Transform (DWT)

Wavelet Transform is a signal processing technique that decomposes a signal or image into different frequency sub bands at number of levels and multiple resolutions. Initially, the input image is decomposed into four levels by a DWT, resulting in an approximation sub band with low frequency components and 12 detail sub bands with high frequency components. The DWT (Discrete Wavelet Transform**)** separates an image into a lower resolution approximation image (LL) as components well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

C. Singular Value Decomposition (SVD)

Another transform domain which is being exploited is Singular Value Decomposition (SVD) due to its simplicity in implementation and attractive mathematical features. It is one of the most powerful numerical analysis technique and used in various applications. Some SVD based algorithms are purely SVD based in a sense that only SVD domain is used to embed watermark into image.

III DIFFERENT APPROACHES FOR WATERMARK EMBEDDING TECHNIQUES

A. A Semi-Fragile Watermarking Approach for Color JPEG Image

The authors [4] proposed a semi-fragile watermarking scheme for colour JPEG image in compressed domain. A chaotic map model based on authentication generating model is introduced. It is sensitive to malicious manipulations and Image authentication is provided to overcome tampering. But it doesn't work for other image formats except JPEG. More number of parameters is used in this approach which occupies more space.

B. Watermark Embedding and Extraction Approach For JPEG2000 Compressed and Encrypted Images

The authors [3] proposed a robust watermarking algorithm used to watermark JPEG2000 compressed and encrypted images. The encryption algorithm used is a stream cipher RC4 approach. In this approach, it embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the decrypted domain. The advantage of this approach is that it preserves the confidentiality of content as the embedding is done on encrypted data and control the image quality as well. But the existing system does not provide compression and encryption schemes for other images.

IV PROPOSED WORK

In the proposed system we first perform pre-processing on the input image and convert it into JPEG –LS format to improve the quality. Watermark embedding is done by using discrete wavelet transform DWT. The watermarked image is again encrypted to provide double security to the original data. The Encryption technique used is Chakra Symmetric Key Encryption, a new approach to encrypt the watermarked image which improves the robustness and Security. The Extraction of watermark can be done in the decrypted domain**.**

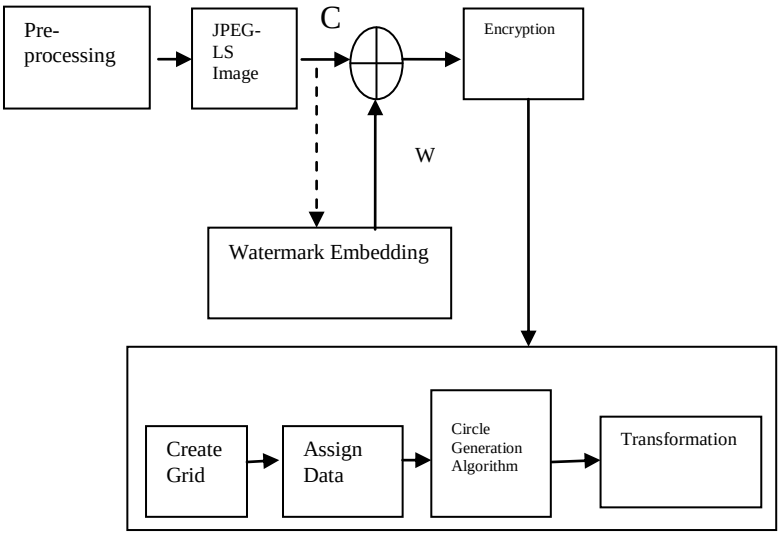


Figure2: Encryption Approach

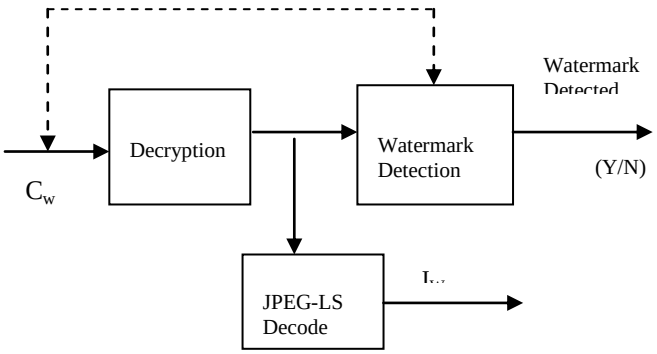


Figure3: Decryption Approach

1. Image Pre-processing

Pre-processing methods use a small neighbourhood of a pixel in an input image to get a new brightness value in the output image. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing[7][8]. In this system we are converting different image formats into JPEG-LS image as JPEG-LS is a lossless compression standard for images and was developed with the aim of providing a low-complexity lossless compression standard that could offer better compression efficiency than lossless JPEG. Lossless image compression attempts to retain absolutely all the information present in the original image.

2. Watermark Embedding

The Discrete Wavelet Transform DWT and Singular Value Decomposition SVD is used to embed watermark in the original image as DWT based algorithms usually produce watermarked images with the best balance between visual quality and robustness due to the absence of blocking artifacts and SVD is used due to its simplicity in implementation and attractive mathematical features.

Watermark Embedding Procedure[6]

Watermark Embedding with 1st Level Decomposition:

Input: Image I=(a_{ij},0≤I,j≤2n) and binary visual watermark W=(w_{ij}€{0,1},0≤i,j≤n).

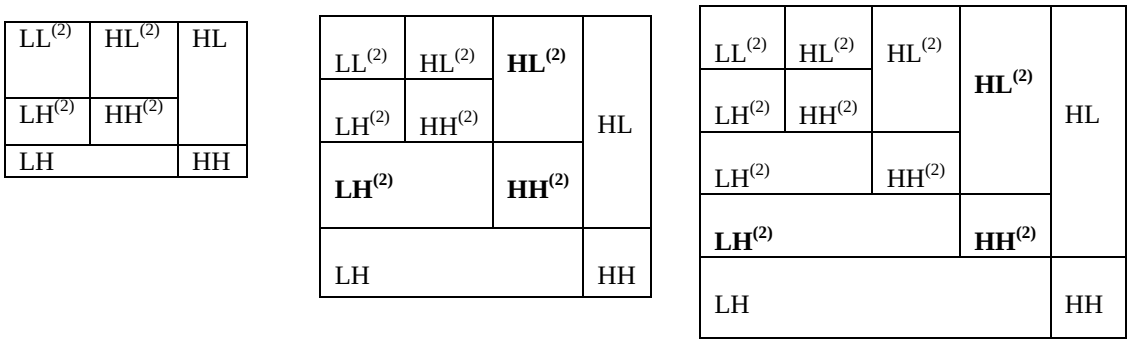
Process:

1. using two-dimensional separable dyadic DWT, obtain the first level decomposition of the cover image I.
2. Modify the DWT coefficients V_{ij} in the LL, HL, LH and HH bands.

$V_{w,ij}^{\ k} = V_{ij}^{\ K} + \alpha_K W_{ij}$,ij=1…..n, and k=1,2,3,4.

3. Apply inverse DWT to obtain the watermarked cover image, I_w.

Output: Watermarked cover image.



(a) Two levels of 2D-DWT (b) Three levels of 2D-DWT (c) Four levels of 2D-DWT

Same process will be done at 4th level Decomposition in our proposed system.

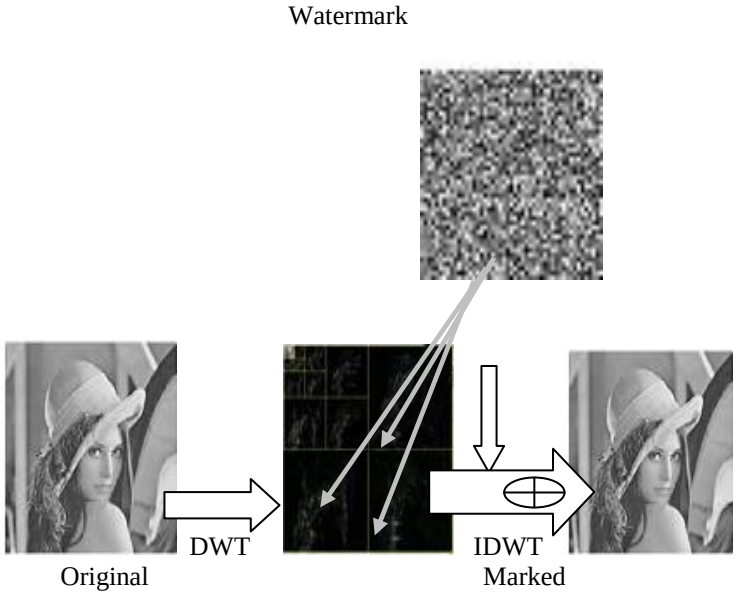


Figure5: DWT Domain Watermarking

3. Encryption Process using CHAKRA – Symmetric Key Approach

The process of converting from plaintext to cipher text is known as Encryption. In this system watermarked JPEG –LS image is encrypted to provide strong security to the original data.

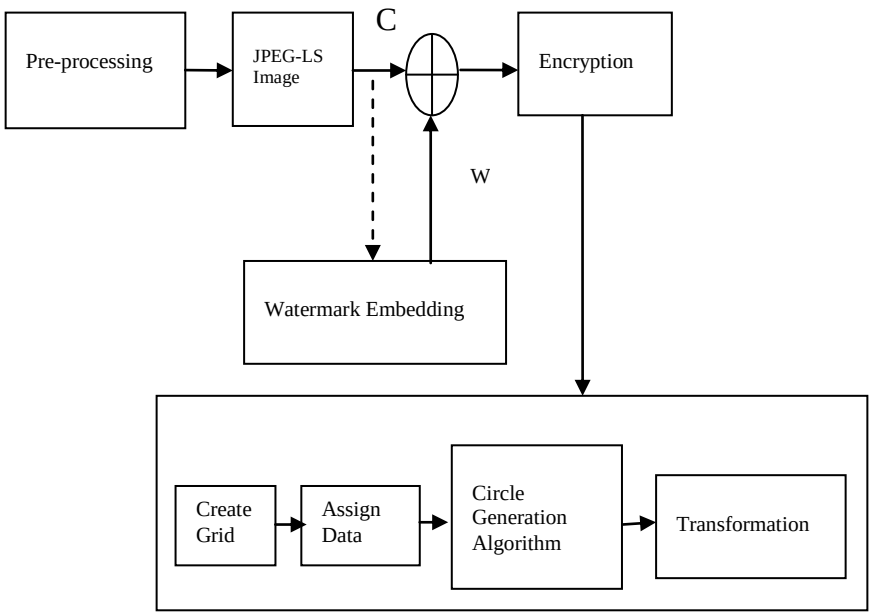


Figure 6:Data Encryption Process

Chakra Algorithm

Chakra Algorithm is a modern symmetric key encryption technique [2] which is used to encrypt the data by using the concepts of Cartesian coordinate and circle transformation (rotation & translation).

When the data is grouped into circles each circle holds the portion of data. The Cartesian axis will be migrated to the respective centers circles and rotated by certain angle. The collection of angle with which each individual circle is rotated; the coordinates to which it is swapped, the size of the square grid the radius of the circle hold the symmetric key. The chakra symmetric key encryption technique consists of the following steps

1. Create Grid
2. Assign data
3. Add noise
4. Generate circles
5. Rotate the circles with random angles add it to the key.

The parameters used are

1. X-Length (XL): Length of the x-axis in the grid.
2. Y-Length (YL): Length of the y-axis in the grid.
3. r: Radius of the circle.
4. Pattern (Pn): The fashion in which the circles in grid are rotated (1-Horizontal, 2-Horizontal snake pattern,3-vertical, 4-vertical snake pattern).
5. Grid: array collection of points (XL*YL).
6. P: Length of bit stream of plain text (bit 0 or 1).
7. Point(x, y, data bit): user defined data class contains x- Coordinate value, y-Coordinate value and Data Bit (binary 0 or 1).
8. Circle: User defined data class contains Circle Center (xc, yc), Coordinate and Coordinate.

Procedure

First we collect the input image and create cartesian grid plain (X_L*Y_L). Add 1 bit of data at every integral cartesian point. Generate random bits at the edge of the grid using Blum Blum Shub Generator to add noise. Generate Circles using Bresenham's circle algorithm with centers. Rotate each circle by angle θ (θ being randomly generated) for each Θ add it to the key(this step) and repeat this step for each circle that exists in the grid, follow the pattern that is given by the user. The obtained data in the grid forms the encrypted image.

3. Decryption Process

The process of converting from cipher text to plaintext is known as Decryption. In this project, Collect all bits from the key, receiver will know what is the pattern size of the grid, pattern selected for encryption, anti-rotate circle by how much angle i.e. rotate by - θ 0 for every θ . Since all are invertible function at the end plain text is achieved.

$$(f'.f)x = f(x)$$

4. Watermark Detection

A watermarked detection unit consists of an extraction unit to first extract the watermark and later compare it with the original watermark inserted. The output is Yes or No depending on whether the watermark is present or not on the image that is being tested.

5. *Watermark Extraction*

After decryption, water mark is extracted and we get original Image.

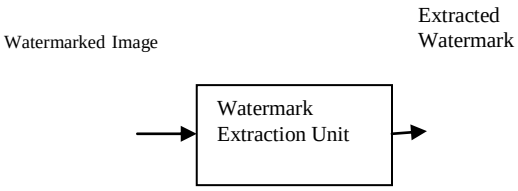


Figure7: Watermark Extraction unit

Watermark Extraction Approach:
Input: Watermarked cover image.
Process:
1. Using two-dimensional separable dyadic DWT, obtain the first level decomposition of the watermarked (and possibly attacked) cover image $I^*_{w.}$
2. Extract the binary visual watermark from the LL, HL, LH, and HH bands:

$W_{ij}^{*} = (V_{w,ij}^{*k} - V_{ij}^{k}) / \alpha_{k,}$ ij=1…..n and *k*=1,2,3,4

3. If $W_{ij}^{*} > 0.5$ then $W_{ij}^{*} = 1$ else $W_{ij}^{*} = 0$

Output: Binary visual watermark

V Conclusion

In this article, we proposed digital image watermarking on different types of images by converting the image format into JPEG-LS, which produces a better result on image transmission through Internet. To provide a two layered security, the watermarked JPEG-LS image is encrypted using Chakra-Symmetric Key Encryption Standard. We believe that this standard two layered protection may deserves the copyright of the owner.

perimental Results

Figure1:Original Image

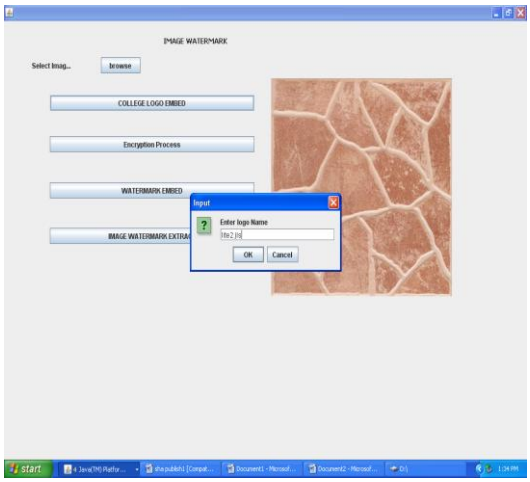


Figure2:Watermark to be Inserted

Figure3:Image after watermark Insertion

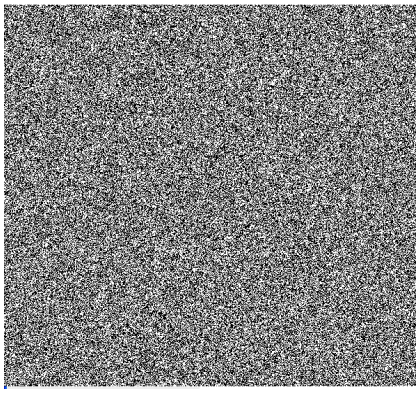


Figure4:Encrypted Image

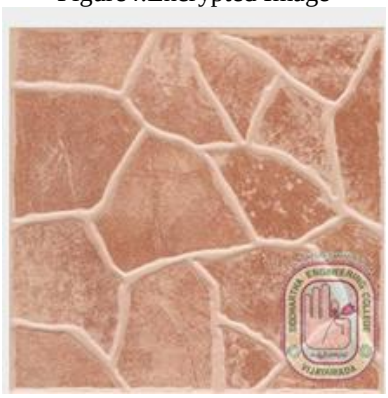


Figure5:Decrypted image

Figure6:Image after Extraction

Figure7:Image after Extraction

References

[1] A.V.Subramanyam,Sabu Emmanuel and Mohan S.Kankanhalli "*Robust Watermarking of Compressed and Encrypted JPEG2000 Images*" in proc.IEEE Int.Conf.Multimedia and Expo.

[2] P.Ramesh Kumar,S.S.Dhenakaran,K.L.Sailaja"*CHAKRA:A New Approach for Symmetric Key Encryption*"in proc.in IEEE 2nd World Congress on Information and Communication Technology,2012,pp-727-732 @2012 IEEE.

[3] A.Subramanyam,SEmmanuel and M.Kankanhalli "*Compressed encrypted domain JPEG2000 Image Waternarking*" in proc.IEEE Int.Conf.Multimedia and Expo,2010,pp.1315-1320.

[4] Qunting Yang "*A Novel Semi-Fragile Authentication Watermarking Scheme of Color JPEG Image in Compressed Domain"* college of Info. Science, Nankai University Tianjin, China.*2010* International Conference on Multimedia Information Networking and Security.

[5] Ensaf Hussein, Mohammed A.Belal"*Digital Watermarking Techniques, Applications and attacks applied to Digital Media: A Survey"*Helwan University, Cairo, Egypt.

[6] Peining Taoa and Ahmet M. Eskicioglub"*A robust multiple watermarking scheme in the Discrete Wavelet Transform domain"* The Graduate Center, The City University of New York, 365 Fifth Avenue, New York, NY 10016 Department of Computer and Information Science, Brooklyn College, The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210.

[7] Alasdair McAndrew *"Introduction to Digital Image Processing with MATLAB*"@2004 by course Technology a part of Cengage Learning.

[8] Madhuri A.Joshi "*Digital Image Processing: An Algorithmic Approach"*@2006 by Learning private Limited,New Delhi.

[9] Chunin Song,Sud Sudirman,Madjid Merabti"*Recent advances and classification of watermarking Techniques in Digital Images"*school of computing and mathematical sciences Liverpool John Moores University,UK.

[10] R. Schyndel, A. Tirkel, and C. Osborne, "*A digital watermark*" in *IEEE Proc. Int. Conf. Image Processing*, 1994, vol. 2, pp. 86–90.

[11] Peining Tao and Ahmet M. Eskicioglu**"***A robust multiple watermarking scheme in the Discrete Wavelet Transform domain"*Department of Computer and Information Science, Brooklyn College, The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210.

[12] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "*Techniques for data hiding"* IBM Systems Journal, vol. 35, no. 3-4, pp. 313-336, 1996.

[13] R.B.Wolfgang and E.j.Delp,"*A watermark for digital images*" in IEEE proc.Int.conf.Image Processing,1996,vol.3,pp.219-222.

