World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

A survey on crypto-enabled watermarking schemes

Kavitha Soppari, Sri Vinay Tanniru *, Sai Teja Gurjala and Rohith Pokala

Department of Computer Science and Engineering ACE Engineering College, Hyderabad, Telangana, India.

World Journal of Advanced Research and Reviews, 2022, 16(02), 887–892

Publication history: Received on 12 October 2022; revised on 18 November 2022; accepted on 21 November 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.2.1254

Abstract

Digital Watermarking is the technique to protect the images, which may be pirated by the other persons. Watermarking is one of the solutions to protect an image, however it is also used to protect audio and video. In watermarking one image is embedded into the image which we want to protect, using certain algorithms, we can't see the embedded image. To increase the robustness and imperceptibility of watermark different variants of algorithms are used. There are different watermarking techniques which have its own advantages and disadvantages. Different algorithms are proposed to increase the robustness and imperceptibility. Cryptosystem concepts are also used in the watermarking to enhance the robustness and security.

Keywords: Watermarking; Robustness; Imperceptibility; Cryptosystem

1. Introduction

Nowadays, technology is growing at a very fast rate and, at the same time, the attacks on our personal data are also increasing. These attacks are not limited to acts such as hacking computers, cracking passwords, stealing personal data, but also pirating images. As images may also contain highly confidential data or are copyrighted, there is a great need to protect the images.

To protect images from such attacks, watermarking is used. Watermarking is the process of embedding a watermark into an image. As these watermarking techniques are available on the internet, it is still possible to separate the watermark from the image. So, watermarking with cryptosystem combination will make watermarking more secure. So, it will be more difficult for the attackers to remove the watermark.

Mostly used cryptosystems are Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), Diffie Hellman Key Exchange (DH).

There are two metrics needed to consider against attacks, which are Imperceptibility and Robustness.

2. Literature survey

However, many researchers proposed different algorithms to maintain perfect levels of imperceptibility and robustness. Maintaining the two factors may not protect the images from attacks, but the effect of an attack on image will be low.

Watermark schemes are classified into spatial domain and transform domain. Transform Domain schemes are robust when compared to spatial domain schemes.

* Corresponding author: Sri Vinay Tanniru
Department of Computer Science and Engineering, ACE Engineering College, Hyderabad, Telangana, India.

Transform domain techniques are categorized as shown in Fig.1.

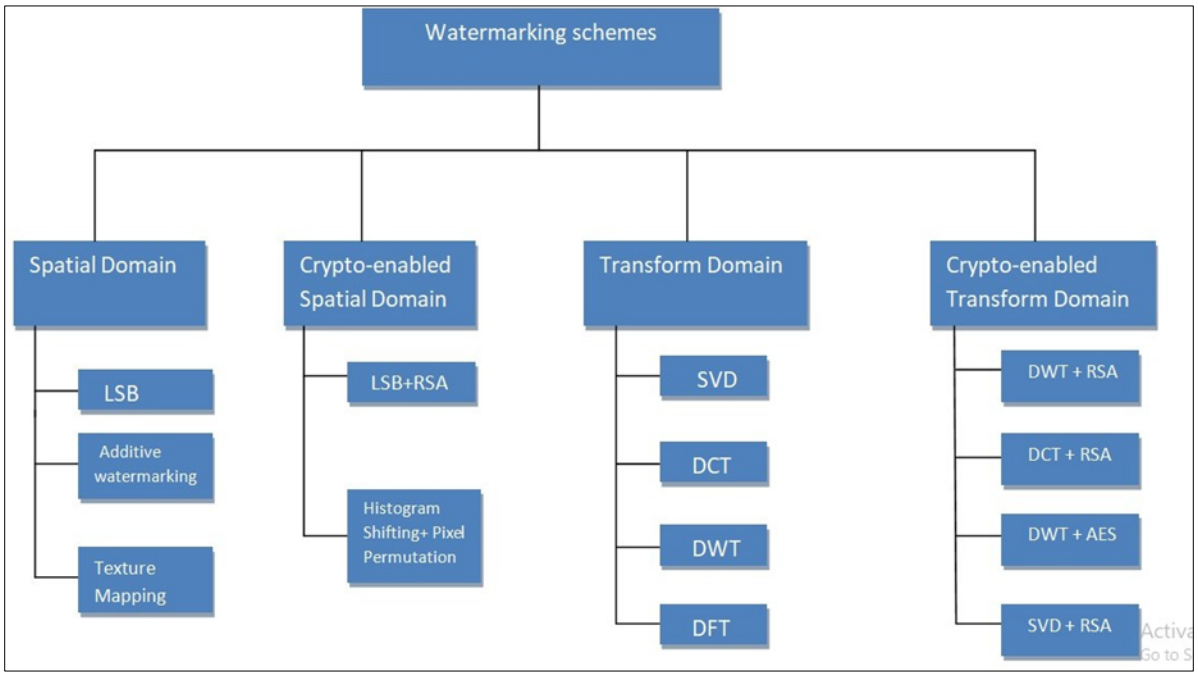

Figure 1 Different Types of Watermarking Schemes

2.1. Spatial domain

[1]In the spatial domain, pixels in randomly selected regions of the images are modified according to the signature. Intensity dithering is done on randomly selected image data.Figure-2 shows the block diagram of spatial-domain data embedding.

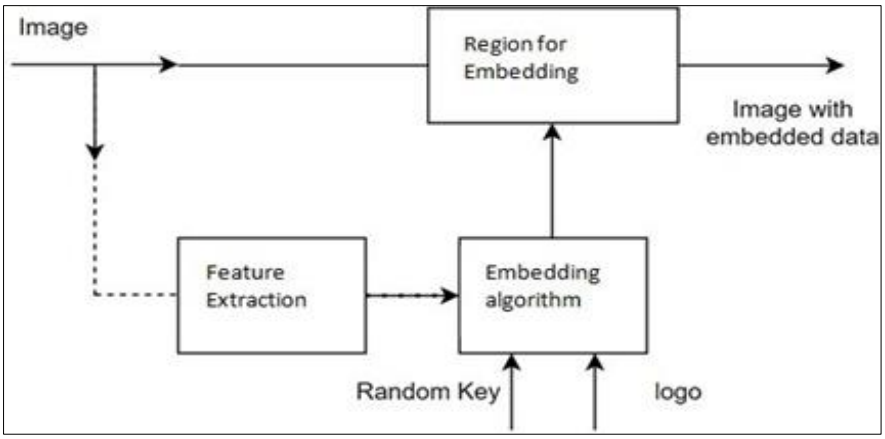

Figure 2 Data embedding

2.2. Transform domains

In spatial domain as the image is directly embedded into the cover image. it can be easily damaged by an attack. Transform domains can reduce the effect of attack. Transform domain techniques can create a perfect balance between the imperceptibility and robustness. But the transform domain techniques are more complex and time consuming to apply. There will not be much difference between the watermarked image and original image.

2.2.1. Singular Value Decomposition (SVD)

The SVD [2] is a mathematic technique used to diagonalize matrices in numerical analysis.

The SVD of an image A with size n x n is given by

$$A = USV^T$$

Where;
U and V are the orthogonal matrices
S is the diagonal matrix. [3]

2.2.2. Discrete Wavelets Transform (DWT)

DWT belongs to frequency domain transformation.

Discrete wavelets transform [4] decomposes the image into four sub bands in a first level decomposition-LL (low-low), LH(low-high), HL(high-low), HH(high-high). The dimension of each sub band is 1/4th of original image. For second level decomposition LL band is further decomposed into LL2, HL2, LH2, HH2.

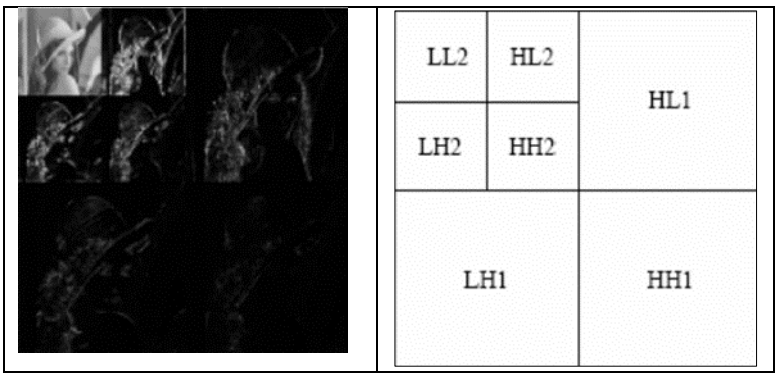

Figure 3 (A)(B)[5] DWT Transformation

2.2.3. Discrete Cosine Transform (DCT)

DCT transform decomposes an image into three frequency bands viz Low Frequency (LF), Medium Frequency (MF) and High Frequency (HF) regions [6] shown in Fig. 4. Medium Frequency regions are chosen for watermarking. Middle Frequency regions offer better resistance to lossy compression techniques than high frequency regions [7].

Different hybrid models of DCT are used to produce robust a d imperceptible watermarking. DCT-SVD, DCT-DWT are examples. By applying DCT, image will be divided into 8x8 or 16x16 blocks.

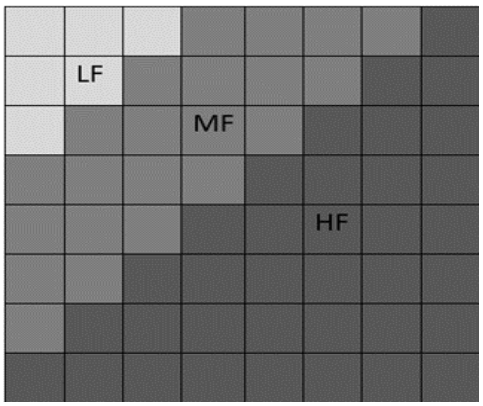

Figure 4 Frequency Bands

2.2.4. Discrete Fourier Transform (DFT)

Most of the researches has proved that DFT domain shows great robustness against geometric attacks. [8] The DFT for the image g (x, y) having M x N pixels is given as:

$$G(u,v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} g(x,y) e^{-j2\pi\left(\frac{vx}{M} + \frac{vy}{N}\right)} \quad (1$$

The inverse of Fourier Transform is given as

$$G(x,y) = \frac{1}{MN} \sum_{u=0} \sum_{v=0} g(u,\breve{y}) e^{j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)} \quad (2)$$

2.3. Cryptosystems

As the watermarking schemes are available on internet, the attackers may have an idea to remove the watermark. So, to provide more protection to the image, encryption concept is used. It will become difficult for the attacker to remove the watermark. Mostly used cryptosystems are RSA, DES, AES algorithms.

2.3.1. Watermarking with RSA Cryptosystem

Rivest-Shamir-Adleman (RSA) is one of the most popular asymmetric public key cryptosystems originated in the year 1978. In RSA a public key is used to encrypt the data and a private key for decrypting the data. Large prime numbers are chosen to generate keys, as factorization of large prime numbers is time taking.

[9] RSA is applied on a 64x64 resolution image and prime numbers are selected randomly between 1 and 200 for every new encryption. For decryption private key is also generated. To get encrypted image watermark, encryption is applied for each pixel of image, then transform domain is applied.

2.3.2. Watermarking with AES Cryptosystems

Advanced Encryption Standard (AES) is approved for the federal us in the United States. As AES is a symmetric, same key is used for encryption and decryption. [10] AES algorithm will have key lengths of 128, 192 or 256 bits and the length of the cipher key is 128, 192 or 256 bits. The key length is represented by 4, 6 or 8 which reflects the number of 32-bits.

Table 1 Different Bit Patterns [10]

Bit Pattern	Key Length	Block Size	No of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

[13]Image is first transmitted into four frequency sub bands, then AES is applied on LL sub band. The reason for choosing the LL-Band for encryption is that most of the image energy is concentrated at lower frequency. AES-128 has been used with 10 rounds. In this the plain text matrix is converted into state matrix by passing through four steps namely Addround key, Subbytes, Shiftrows and Mix columns.

2.3.3. Watermarking with DES Cryptosystem

Data Encryption Standard (DES) algorithm is a symmetric cryptosystem and comes under the block cipher. In DES the 64-bit plain text will be encrypted to 64-bit cipher text.

[11] In the First step, the plain text block is mutated with the initial permutation matrix. In the second step the initial permutation results are then encrypted 16 times. In the third step the encoding results are mutated with the initial inverse permutation matrix into a cipher text block. [15] Image is decomposed by two level DWT (N x N) and a random key "K" of 64 bits is generated. Image is divided into binary watermark image ofsize.

((N x N)/4) in blocks of size 8 x 8. These image blocks are encrypted using key "K" and encrypted image blocks are appended to form complete watermark image.

3. Review on different algorithms

Table 2 Review on Different Watermarking Algorithms

Author	Domain	Cryptosystem	Review
Bidyut Jyoti Saha, Chittaranjan Pradhan, Kunal Kumar Kabi, Ajay Kumar Bisoi [12]	DWT	RSA	Doubly encrypted watermarking is used. In this RSA encryption is applied to the whole image, so the decryption time exponentially increases with the RSA parameters.
V.Chandra Prasad, S.Maheswari[13]	DWT, DCT	AES	In this only particular region of image is selected for encryption. Hence computation time is reduced.
Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma [14]	DWT, SVD	RSA	This experiment demonstrated better robustness,less encryption time and large data embedding capacity.
N. Tiwari, M. K. Ramaiya, and M. Sharma [15]	DWT	DES	Because of block size limitation of DES, the image has to split into 8x8 blocks before encryption,this makes encryption ad decryption process inefficient for larger images
A. Joshy, and N. Suresh[16]	DWT	AES	As the watermark is binary coded decimal, it makes AES encryption efficient. This experiment shown a decent level of imperceptibility, but robustness was not evaluated.
Koushik Pal, Subhajit Koley, Goutam Ghosh, Mahua bhattacharya [17]	DCT	RSA	Different image quality metrics are measured and the results are good. As it deals with medical images, it requires much care during embedding and extracting the information
Y.Bhavani,Sai Srikar uppala, Spoorthy Shivani Pabba, Kavya Sri Kasarla [18]	DWT, SVD	RSA	DWT is applied on cover image, then the segmented watermark image is embedded into cover image with SVD, then RSA is applied to the whole image, this algorithm can also be extended to color images.

4. Conclusion

The two metrics needed to be considered in watermarking are Robustness and Imperceptibility. In this paper, various algorithms offering various levels of robustness and Imperceptibility are studied. Cryptosystem enabled algorithms enhance the security levels in watermarking schemes. However, applying cryptosystems in image is a challenge as images contain large data. This paper gives an overview on different watermarking schemes. Different Hybrid algorithms (crypto-enabled and non-crypto algorithms) are given brief in this paper.

Compliance with ethical standards

Acknowledgments

We would like to thank our guide Mrs. Soppari. Kavitha for her continuous support and guidance. Also, we would like to express our gratitude to Dr. M.V.VIJAYA SARADHI, Head of the Department of Computer Science and Engineering, Ace Engineering College who was a continual source of inspiration.

Disclosure of conflict of interest

We have no conflicts of interest to disclose. All authors declare that they have no conflicts of interest.

References

[1] W.N. Cheung, “Digital Image Watermarking in Spatial and Transform Domains.”

[2] Ruizhen Liu and Tieniu Tan,”An SVD-Based Watermarking Scheme for Protecting Rightful Ownership.”

[3] Jing Liu, Douli Ma, Yajie Yang “A New Singular Value Decomposition Watermarking Algorithm Based on Direction let. “

[4] Vibha Verma, Vinay Kumar Srivastava, Falgun Thakkar “DWT-SVD based Digital Image Watermarking using Swarm Intelligence.”

[5] Sebile AYDIN, Merve MEMİŞ, Dr.Ersin ELBAŞI “Digital Image Watermarking Method in Multi-Level DWT.”

[6] Jobin Abraham and Dr. Varghese Paul “Image Watermarking using DCT in Selected Pixel Regions.”

[7] Tribhuwan Tewari and Vikas Saxena “An Improved and Robust DCT based Image Watermarking scheme.”

[8] Akshay K Kallianpur, Bharath M V, Manikantan K “Digital Image Watermarking Using Optimized Transform-Domain Approach.”

[9] P.V.V. Kishore, N. Venkatram, Ch.Sarvya, L.S.S.Reddy “Medical Image Watermarking using RSA Encryption in Wavelet Domain”.

[10] M.Pitchaiah, Philemon Daniel, Praveen “Implementation of Advanced Encryption Standard Algorithm.”

[11] Rismayani, Cucut Susanto “Using AES and DES Cryptography for System Development File Submission Security Mobile-Based.”

[12] Bidyut Jyoti Saha, Chittaranjan Pradhan, Kunal Kumar Kabi, Ajay Kumar Bisoi “Robust Watermarking Technique using Arnold’s Transformation and RSA in Discrete Wavelets .”

[13] V.Chandra Prasad, S.Maheswari” Robust Watermarking of AES Encrypted Images for DRM systems.”

[14] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, “Secure and Robust Digital Image Watermarking Scheme using Logistic and RSA encryption.”

[15] N. Tiwari, M. K. Ramaiya, and M. Sharma, “Digital watermarking using DWT and DES”

[16] A. Joshy, and N. Suresh, “A Dual Security Approach for Image Watermarking using AES and DWT.”

[17] Koushik Pal, Subhajit Koley, Goutam Ghosh, Mahua bhattacharya “A new Combined Crypro- Watermarking Technique using RSA algorithm and Discrete Cosine Transform to Retrieve Embedded EPR from Noisy Bio-Medical Images.”

[18] Y.Bhavani, Sai Srikar Puppala, Spoorthy Shivani Pabba, Kavya Sri Kasarla “Image Segmentation Based Hybrid Watermarking Algorithm for Copyright Protection.”

[19] Muhammad Khairi Abdul Razak,Kamilah Abdullah, Suhaila Abd Halim “A Review on Digital Image Watermarking With Cryptosystem Techniques.”

[20] Kavitha Soppari, N. Subhash Chandra “Development of improved whale optimization-based FCM clustering for image watermarking.”