ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

A Review of Watermarking Algorithms for Digital Image

Jaishri guru[1], Hemant damecha[2]

[1] Student of M.E. Software Systems, Department of Computer science and Engineering, Shri ram Institute of Technology, Jabalpur (R.G.P.V University Bhopal), Madhya Pradesh, India

[2]Assistent Professor, Shri ram Institute of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT: The growth of the Internet along with the increasing availability of multimedia applications has spawned a number of copyright issues. One of the areas that this growth has fueled is that of digital watermarking. Digital watermarking is the general technique of embedding a blob of information in the original file, such that an altered file is obtained. The blob of information, thus included, serves one of different uses, such as, identifying piracy, sensing tampering, or reassuring integrity. The approaches to watermarking are diverse and can be broadly classified based on their visibility, robustness, or fragility. Their uses are also versatile, as they can be applied to text, images, audio, or video. In this paper, we will go through various algorithms of watermarking for digital image.

KEYWORDS: Digital watermarking classification, SVD, DCT, DWT, HVS.

I. BROAD CLASSIFICATION OF WATERMARKING TECHNIQUES

I. Watermarking techniques can broadly be classified based on their inherent characteristics: visible and invisible [1].

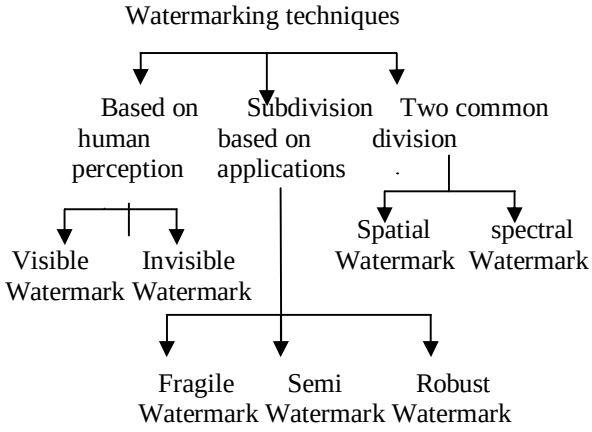

Figure 1: Broad classification of watermarking techniques [2]

Visible watermarks: A visible alteration of the digital image by appending a "stamp" on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.

Invisible watermarks: By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non-repudiation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

II. Another way of classifying watermarking technique is a factor of its usage: fragile, semi-fragile, and robust [3].

Fragile watermarks: These are complementary to robust watermarks and are, as a rule, more change-sensitive than robust watermarks. They lose their mettle when they are subject even to the smallest changes. Their use lies in being able to pin-point the exact region that has been changed in the original watermarked image. The methods of fragile watermarking range from checksums and pseudo-random sequences in the LSB locate to hash functions to sniff any changes to the watermark [4].

Semi-fragile watermarks: These watermarks are a middle ground between fragile watermarks and fragile watermarks. They engulf the best of both worlds and are more resilient than fragile ones in terms of their robustness. They also are better than robust watermarks in terms of locating the regions that have been modified by an unintended recipient.

Robust watermarks: By hypothesis robust digital watermark repeal all types of attacking techniques on the watermark [5]. Watermarks can be used to hold knowledge of ownership. Such watermarks need to remain steadfast to the original image to do what they advertise. The intactness of the watermark is a measure of its robustness. These watermarks must be able to withstand normal manipulations to the image such as reduction of image size, lossy compression of image, changing the contrast of the images, etc.

III. Digital watermarks are also spatial and spectral watermarks.

Spatial watermarks: Watermarks that are applied to the "spatial domain of the image" are said to be spatial watermarks [6].

Spectral watermarks: These are watermarks that are applied to the "transform coefficients of the image" [6].

The rest of the paper is organized as follow. The ground rules for a good watermark will be laid down in the next section. After describing the various stages of the watermarking process, we will focus on various algorithms for watermarking, and analyze the algorithms.

Criteria for a good watermark:
Though watermarks belong to different categories, some of the general characteristics that watermarks must possess are the following [7]:

1. The watermark must be strongly bound to the image and any changes to the watermark must be apparent in the image.
2. Watermark must also be able to withstand changes made to the image. Such changes include modifications and enhancements of images such as size modifications, cropping, and lossy compression, to name a few.
3. The watermark must not undermine the visual appeal of the image by its presence (especially for invisible watermarks).
4. Watermark must be indelible and must be able to survive linear or non-linear operations on the image [8].

The following are criteria for a visible watermark: [9]

1. The watermark must be apparent on all kinds of images.
2. The size of the watermark is crucial. The more pervasive the watermark the better so that the watermarked area cannot be modified without tampering with the image itself.
3. The watermark must be fairly easy to implant in the image.

The Watermarking Process
The watermarking process comprises of the following stages [10].
1. Embedding stage
2. Extraction phase

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

3. Distribution stage
4. Decision stage

Embedding stage: In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients [11].

Distribution stage: The watermarked image obtained above is then distributed through digital channels (on an Internet site). In the process, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a few. Peter Meerwald [11] refers to the above as "coincidental attack". Any of the above may put the watermarking scheme to test, as we will see in the ensuing section. In addition, malicious attacks also are possible in this stage to battle with the watermark. These are referred to in Meerwald's work [11] as "hostile attacks".

Extraction stage: In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image [11].

Decision stage: In this stage, the extracted watermark is compared with the original watermark to test for any discrepancies that might have set in during distribution. A common way of doing this is by computing the Hamming distance [11].

$$HD = \frac{(W^{mod.}\ W)}{\|W^{mod}\|.\|W\|}$$

Where, both the numerator and the denominator are the dot products.
HD obtained above is compared to a threshold, T, to determine how close W^{mod} is to W.

II.LITERATURE REVIEW: TECHNIQUES USED IN WATERMARKING FOR DIGITAL IMAGES

Digital watermarking is a technology that manages and assigns data authentication, security, and copyright security to the digital information. Digital watermarking algorithms are divided into two groups. One technique is spatial domain. In this techniques pixel values straightly works. The Second is frequency domain techniques employ several transforms, either local or global. Various widely recognized techniques are described consequently [12].

Spatial Domain Techniques: Watermark in spatial domain technique is inserted in the cover image and changing pixels value. Against the possibility of the watermark becoming visible the algorithm should carefully weight the number of altered bits in the pixels value [12].

Frequency Domain Techniques: Frequency-domain methods are more widely applied as compared to spatial - domain methods. The aim of watermarks in the spectral coefficients of the image is embedded. In frequency domain Mostly used transforms are the **DCT** (Discrete Cosine Transform), **DFT** (Discrete Fourier Transform), **DWT** (Discrete Wavelet Transform).For as much as the characteristics of the **HVS** (human visual system) are better captured by the spectral coefficients that's why watermarking in the frequency domain. For example, human visible system for low-frequency coefficients is more sensitive, and for high-frequency coefficients it is less sensitive, also we can say that in troths, The LF (low frequency) coefficients are significant perceptually, that means distortion in the original image might cause by those components and high-frequency coefficients are insignificant considered. Thus, HF (high frequency) coefficients aggressively remove by processing techniques like compression. To get a balance between robustness and imperceptibility large algorithms embed watermarks in the midrange frequencies [13].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

Discrete wavelet transform: Discrete wavelet transform **(DWT)** is a neoteric technique consecutive used in digital image processing, compression, digital watermarking etc [14]. Discrete wavelet transform is more efficient than discrete cosine transform method. The image is dissolved into high and low frequency elements in two level discrete wavelet transform (DWT). The robustness with respect to divers attacks increases when the watermark is embedding in low frequencies gained by WD (wavelet decomposition). Now first digital media is segmented into frames, Then discrete wavelet transform is applied to luminance element of each frame which outcomes into discrete sub bands. Again these bands are dissolved into discrete components. Now covariance matrix is calculated for each component. Now watermarked luminance component of the frames are gained by applying inverse discrete wavelet transform. Ultimately watermarked digital media is gained by renewing the watermarked frame [14, 3].

Singular value decomposition: Singular value decomposition is a rousing numerical technique which is utilized to diagonally matrices in numerical analysis [15]. In variety of applications singular value decomposition is used as an algorithm. In this singular value decomposition transformation, One matrix can be dissolved into three matrices. These matrices are of the equal size as the original matrix. By the linear algebra, an image is an array of nonnegative entries of scalar values that can be deduced as a matrix. Sine tort of important component, Assume if formula is $A \in R^{m*n}$ where A is a square image, R is the real number domain, Then singular value decomposition of A is denoted as $A = USV^T$. Here U and V both are orthogonal matrices, and diagonal matrix is S, as

$$S = \begin{pmatrix} S1 & . & \\ & . & \\ & & Sn \end{pmatrix}$$

Here diagonal components i.e. s's are singular values and satisfy S1≥S2≥…....Sr≥Sr+1≥==……..=Sn==0
Singular value decomposition is an optimal matrix decomposition technique in a least square sense that it grids the highest signal energy into some coefficients as feasible [16].

Hash Functions as fragile watermarks:
According to Wolfgang and Delp's [17], hash functions can be used as fragile watermarks. One of the methods they have used as watermarks is the block-based hash function (BBHF) [17]. The hash is computed on the width and height of the image block. Specifically, X_b is the width of the block and Y_b is the height of the block and $X_b * Y_b$ is the hash function. The hash values of every block of the image are stored. In order to test the sanctity of an image, the stored hash values are compared to the hash values of the image whose sanctity is to be tested. If the hash values do not correspond to each other, then the block which houses the discrepancy is the one that has been altered.

Figure 2: test image for a modified image using BBHF from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf

Variable-Watermark Two-Dimensional Algorithm (VW2D) [17]
Wolfgang and Dr. Delp's have developed this algorithm for image authentication. Both the watermark and the watermarked image are used here to authenticate the image. A pseudorandom binary sequence is the watermark and this sequence is superimposed on the original image in blocks. This can be elucidated as follows:
Let WI be the watermarked image, W be the watermark and X be the original image. Then WI_b is a block of the watermarked image, W_b is a block of the watermark and X_b is a block of the original image. The watermarked image is generated as follows [17]:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

$WI = WI_{b1} + WI_{b2} + \ldots + WI_{bn}$

And each watermarked image block is generated as follows:

$WI_{bi} = X_{bi} + W_{bi}$ (where I = 1 to n)

Checking to see if a watermark resides in an image (Test) is done as follows:

$_{bi} = W\Delta_{bi} . W_{bi} - Test_{bi} . W_{bi}$

A threshold value can be chosen to authenticate the test image. The threshold is compared with the delta value computed above. The choice of the threshold value can determine the extent of changes that are tolerated to the watermarked image. The spectrum of scenarios that can be tested range gradually from unchanged to highly manipulate. Such a choice also gives the users of this algorithm some leeway in choosing the strictness with which manipulations are caught. The effect of choosing different threshold values can be seen in the images in the Appendix (Figures 3, 4, 5, 6).

Figure 3: Original image (before watermarking) obtained from

Figure 4: Watermarked image using the VW2D algorithm.

Figure 5: test image for a modified image using VW2D with a threshold T =0 from

Figure 6: test image for a modified image using VW2D with a threshold T=200 from

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

II. HUMAN VISUAL SYSTEM (HVS)

In order to develop good watermarking algorithms, characteristics of the human visual system have been extensively studied. The nuances of visual perception have given scientists an insight into modeling watermarks that do not interfere with the host image. Wolfgang, Delp and Podilchuk [17, 8] have listed some of the characteristics of the human visual system by the following 3 criteria, as given in Wolfgang et al's paper [17, 8]:

1. Sensitivity to frequency: The HVS is more sensitive to higher frequencies than to lower frequencies. [17,8]
2. Contrast masking: This refers to how one signal influences the expression of another signal. Presence of two signals in the same frequency enhances this property [17, 8].

While the above two algorithms have been applied to the spatial domain of the image, watermarking algorithms that tap into various transforms became popular, thanks to their robustness and quality. Some of the transforms that are used for this purpose include the DCT (discrete cosine transform), DFT (discrete Fourier transform) and the wavelet domains. These techniques combined with studies on the human visual system have allowed for the development of good watermarking techniques.

A very popular compression technology for still images is JPEG [17,8]. Compression in JPEG occurs as follows. The still image to be compressed is passed through a coder, which transforms the image by ripping it into distinct blocks of 8*8 pixels. A DCT is applied on the thus obtained distinct blocks.

A Semi-Fragile Watermark in the DCT domain –Lin's algorithm:

Lin's et. al [18] has developed a semi-fragile watermark in the DCT domain.

Watermark: The watermark is given by "pseudo-random zero-mean, unit variance Gaussian distributed numbers" [18]

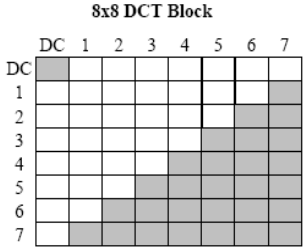

Figure 7: watermarking process using the DCT domain.

In the figure 7, clear blocks are marked coefficients while the grey blocks are unmarked coefficients. Figure obtained from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf

Embedding stage: Watermark is embedded in every 8*8 DCT block. Though each block has a different watermark, the watermark is embedded on the same indices of each block. The DC coefficient and some other coefficients including the high frequency AC coefficients of the block are not marked. The inverse DCT is constructed to produce the watermark W. [18]

WI= O + strength (W),

Where, WI is the watermarked image, O is the original image, and strength is the strength of the watermark.

Detection stage: Detection is done by comparing blocks with corresponding blocks to localize any changes. A threshold is compared to the test value computed for each of the blocks to figure out if a block has been modified. The algorithm described in Lin's paper is discussed below. [18]

Let B(x, y) be an arbitrary block.

Col-diff (Block(x, y)) = Block(x, y) – Block(x+1, y) for x in {1, 2,…blocksize –1) or
0 if x = blocksize

Row-diff (Block(x, y)) = Block(x, y) – Block(x, y+1) for y in {1, 2,…block size –1) or

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

0 if y = block size

T is computed as a single matrix obtained by concatenating col-diff and row-diff of the test image block and water-block is the corresponding matrix for the watermarked image.

T = [Col-diff (T(x, y)) Row-diff (T(x, y))]

W = [Col-diff (W(x, y)) Row-diff (W(x, y))]

Since we need to obtain a dot product, the matrix T and W above are permuted to obtain a vector. The permutation function, F, should be uniform for both the matrices.

F (T) = vector (T)

W (T) = vector (T)

The test statistic, S, can be computed as follows:

S = (T.W) / sort ((T.T) (W.W))

Comparing the blocks can be done as follows. An appropriate threshold, T, is chosen and compared with the test statistic.

S >= T => block unaltered

S < T => block altered

VI. EVALUATION OF ALGORITHMS

The hash algorithm and the VW2D algorithms were used in the spatial domain while Lin's algorithm utilized the DCT domain. The hash algorithm is the least tolerant to changes to images, while both VW2D and Lin's algorithm offered some resilience to change in the form of a tolerance level that could be assigned for comparisons. However, while both VW2D and Lin's algorithm can handle lossy compression that JPEG doles out to images, Lin's algorithm also made use of the HVS perception in its algorithm by only making changes to the low frequency coefficients. Since JPEG compression is done using the DCT transform, Lin's algorithm is the best bet for JPEG images. Using any of the above algorithms will reflect changes made to the watermarked images, although to different extents. The watermarks themselves are not too difficult to embed and hence can be embedded easily. An appropriate watermarking process can therefore be chosen, based on the purpose and level of protection required.

V.CONCLUSION

Watermarking is a vast field and a lot of research is going on in this area. There are commercial players who are vying for dominance in this field. Though a clear-cut winner has not been declared yet, a combination of other cryptographic techniques (such as encryption) and watermarking together will definitely provide copyright protection for images. Depending on the intended requirements and the level of security required, an appropriate watermarking algorithm can be chosen.

REFERENCES

1. Gaurav Chawla, RaviSaini, Rajkumar Yadav, Kamaldeep, "Classification of Watermarking Based upon Various Parameters", International Journal of Computer Applications & Information Technology Vol. I, Issue II, September 2012 (ISSN: 2278-7720).
2. Jaishri Guru, Hemant Damecha, "Digital Watermarking Classification : A Survey", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, pp.8-13, Sep-Oct 2014.
3. Neha Rawat, Rachna Manchanda, "Review of Methodologies and Techniques for Digital Watermarking", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 4, pp. 237-240, April 2014.
4. E. T. Lin and E. J. Delp, "A Review of Fragile Image Watermarks," Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents, Orlando, pp. 25-29, October 1999.
5. Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S," A RESEARCH REVIEW ON DIFFERENT DATA HIDING TECHNIQUES", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 1, Page No. 3655-3659, Jan 2014.
6. Sonya Inna Lyatskaya, "DIGITAL WATERMARKING TECHNIQUES IN IMAGE PROCESSING**",** M.S. Alabama A&M University, 140 pp, 2006.
7. http://www.acm.org/~hlb/publications/dig_wtr/dig_watr.html
8. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1108-1126, July 1999.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

9. http://www.cs.unt.edu/~smohanty/research/ConfPapers/2002/MohantyICME2000.pdf
10. Potdar, V.M.; Song Han; Chang, E., "A survey of digital image watermarking techniques," Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference on, vol., no., pp.709, 716, 10-12 Aug. 2005doi: 10.1109/INDIN.2005.1560462.
11. Peter Meerwald and Andreas Uhl, "Digital Watermarking in the Wavelet Transform Domain", January 2001.
12. Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme", International Journal of Engineering Research,Volume No.2, Issue No.3, pp : 193-199, 01 July 2013.
13. Pravin M. Pithiya,"DCT Based Digital Image Watermarking, Dewatermarking & Authentication", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 3 May 2013,page no. 213-219.
14. Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images".
15. Sangeeta Madhesiya,Shakil Ahmed, " Advanced Technique of Digital Watermarking based on SVD-DWT-DCT and Arnold Transform", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, page no. 1918-1923, May 2013.
16. Mohammad Ibrahim Khan, Md. Maklachur Rahman and Md. Iqbal Hasan Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT,DWT and SVD Transformation".
17. R. B. Wolfgang and E. J. Delp, "Fragile Watermarking Using the VW2D Watermark," Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, pp. 204-213, January 25 - 27, 1999.
18. E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of Image Alterations Using Semi-Fragile Watermarks," Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II, Vol. 3971,San Jose, CA, January 23 - 28, 2000.

BIOGRAPHY

Miss jaishri guru received her B.E. in CSE from Takshshila institute of engineering and technology (R.G.P.V.Bhopal),Madhya Pradesh, India in 2011.Currently she is pursuing M.E. in Software systems from S.R.I.T (Affiliated to R.G.P.V,Bhopal). She is working on project related to "DIGITAL WATERMARKING". Her interest areas are Digital Image Processing, Network security and Network Management.