A Survey on Digital Watermarking and its Application

Ms.Mahua Pal
J.D.Birla Institute
Jadavpur University
Kolkata, West Bengal, India

***Abstract*—Digital communication plays a vital role in the world of Internet as well as in the communication technology. The secrecy of the communication is an essential part of passing the data or information. One noticeable technique is Digital Watermarking. Copyright owners seek methods to control and detect such reproduction, and henceforth research on digital product copyright protection has significant practical significance for E-commerce & E-Governance. In this paper, a survey on some previous work done in watermarking field is presented. Experimentally evaluated algorithms are collected to focus on the wide scope of encrypted digital watermarking for data transmission security and authentication.**

***Keywords*—Watermarking; Watermarking technique; DCT; DWT; LWM; DFRNT; PSNR**

I. INTRODUCTION

Digital Watermarking started back in 1979, but it was not until 1990 that it gained popularity. Its full-fledged application began around 1998. No one is credited with founding or inventing the digital watermark, still it is in its growth stages today, and with cases like Napster, it is showing more and more reasons to have digital watermarking.[12] Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography. But unlike steganography, watermarks typically hide very little information and rely on the part on redundancy of the mark to survive attacks such as cropping. Digital watermarks contain information that may be considered attributes of the covering image such as copyright data, and the cover is the object of communication - not the watermark. It is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information unique to the copyright owner, the creator of the document or the authorized consumer. Watermarking leaves the original file/ image intact and recognizable.

Watermarks are embedded into images by changing some bits in image representation. The original data (payload) is first encrypted and watermarked in encoder (sender) and then sent to a decoder (receiver) through the internet to be decrypted and extracted. The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, colour correction, or geometric modifications. Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks. Imperceptibility means the watermark is not seen by the human visual system. Complexity is described as the effort and time required for watermark embedding and retrieval. Lastly, verification is a procedure whereby there is private key or public function (Dittmann, Mukherjee & Steinebach, 2000). Each of these properties must be taken into consideration when applying a certain digital watermarking technique. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others.[13]

Current image-based digital watermarks may be grouped under two general classifications: those that fall into the *image domain* and those that fall into the *transform domain*. These techniques of watermarking are applied to graphic images and text. i) *Image domain* is also called spatial domain watermarking that slightly modifies the pixels of one or two randomly selected subsets of an image. However, this technique is not reliable when it is subjected to normal media operations such as filtering or lossy compression (Berghel, 1998). ii) *Frequency domain* watermarking technique is also called transform domain. Values of certain frequencies are altered from their original to the lower frequency levels. These techniques of watermarking are applied to graphic images and text.

The Zhao Koch Algorithm and The Fridrich Algorithm watermark techniques are applied to MPEG videos. The Zhao Koch Algorithm embeds a copyright label in the frequency domain of the video. The watermark can be easily embedded into the video with minimal operation. The Fridrich Algorithm watermark technique is where a pattern is overlaid in the low frequency domain This watermark technique does not include detail information about the owner when the pattern is created and overlaid, so verification using this algorithm is not reliable. This algorithm is resistant to normal media operations whereas the Zhao Koch Algorithm watermark technique is not robust against normal media operations such as scaling or rotation (Dittmann, Stabenau & Steinmetz, 1998).

Few research works on digital watermarking are discussed in the subsequent section.

II. LITERATURE REVIEW

A. Peyman Rahmati, Andy Adler and Thomas Tran (2013) , "Watermarking in E-commerce" [3]. In this paper a technique is proposed to protect digital identity documents against a Print Scan attack for a secured ID card authentication system. The existing PS operation imposes several distortions, such as geometric rotation & histogram distortion on the watermark location which may cause the loss of information. The proposed system removes distortion of the PS operation: - filtering, localization, binarizitation, rotation and cropping. The proposed authentication system extracts the watermarks inside the ID card's holder photo, place in the decoder and then checks it out with the ID card personal number. If the extracted watermark and the ID card personal number are the same, the identity of the user / customer will be verified otherwise identity will be denied. A decision function for extracting a bit of the hidden data at the position (i, j) can be written as:

$d(i,j) = Corr(B^{W}ij(k,l), f1(k,l)) - Corr(B^{W}ij(k,l), f0(k,l))$, where $B^{W}ij(k,l)$is the block in the watermarked image; f1 , f0 are the Hadamard pattern used in encoder. The decision function to find the binary hidden data at the position (i j)is $W(i,j) = sgn (d(i,i)) = +1$ if x = 1

$$\begin{cases} -1 & \text{if } x = 0 \end{cases}$$

where W(i,j) is a bit of the binary hidden data at the position (i,j).

B. Neil F. Johnson, Zoran Duric and Sushil Jajodia, "A Role for Digital Watermarking in Electronic Commerce". [1] In this paper, a new way of categorizing watermark technique through image modeling is discussed. The image modeling called 'alpha channel composition' uses gradual mask. Two images with flat mask and gradual mask are used to create watermark that changes gray values of pixel in the image. A method of watermark recovery by applying inverse transformation to the distorted images is shown. The image is watermarked using the version of Digimarc's PictureMark watermarking filter that is available with Adobe PhotoShop and the image is distorted by applying the Stirmark tool of affine transformation.

C. Swathi.K, Ramudu.K (2014), "Robust Invisible QR Code Image Watermarking Algorithm in SWT Domain"[2]. A binary image is the watermark here. In the frequency domain, the embedding process on QR code image using watermark is performed. The QR code image is decomposed by one level using one dimensional wavelet transformation. To restore the embedded watermark there is no need of the original QR code image. The secret key for embedding and extracting of the watermark is the pseudo-random sequence (P) where each number can take a value either 1 or -1, randomly generated.

$P = \{ pi , 1 \leq I \leq N\}$, pi {-1, 1}, where N is the total number of pixels in the watermark image.

The robustness of the algorithm with some attacks such as Salt and Pepper noise, Gaussian noise, and Scaling and Rotating shows extracted watermark with difference magnitude factors. All extracted watermark images contain some visual noise because of the watermark extracting process did not employed the original QR code image

D. Vinita Gupta, Atul Barve(2014), "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes"[4]. In this Paper, algorithm for embedding watermarking is presented by using DWT and encrypted with QR codes. Here cover image is selected and DWT is applied on it. A key K is selected to generate the QR code as secret key. QR code and watermark image is encrypted by using XOR operation. Then the encrypted watermark is embedded into the cover image and inverse DWT is applied on the embedded watermark image. For extraction, simply apply the DWT on the cover image. This algorithm is quite simple because of the use of simple X-OR operation for encryption. This algorithm is suitable on different kind of attacks on watermarked images like JPEG Compression, Possion Noise Attack, Salt & Pepper Noise and Gaussian Noise.

E. M. Kim, D. Li, and S. Hong(2013), "A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents" [5]. In this paper, algorithm for embedding watermarking is presented. Firstly, the original image is compressed into JPEG image and generates the watermark by using the 2D barcode and scrambling. Secondly, JPEG image is decayed into 3 sub-bands: H, V and D by using 2D DWT. Thirdly, the DFRNT(discrete fractional random transform) is performed on the sub-band coefficients. And then, watermark image is embedded into the sub-band coefficient value using quantization technique. Fourthly, the inverse DFRNT and inverse DWT is performed and lastly watermark JPEG image is obtained. The proposed algorithm has good invisibility and extraction performance, and ensures robustness.

F. Arathi Chitla, M. Chandra Mohan(2012), "Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)"[6]. In this paper, a method for authenticating the image using lossless water marking is being proposed that offers high capacity host signal (information) and non-altered image by implementing the elliptic curve cryptography and LSB method. The proposed LWM image authentication technique involves of four processing stages namely, i) information authentication, ii) data embedding on image, iii) information and image recovery, and iv) verification. These four stages are consecutively performed and thus obtained the watermarked and recovered images. A novel lossless watermarking image authentication technique is proposed in this paper. The technique provides high embedding capacities, allows complete recovery of the original host signal, and the retrieved image have high PSNR value than the conventional technique. The PSNR value of the recovered image proved that the image was not altered and the

lossless watermarking procedure was successfully implemented.

G. Shraddha S. Katariya(2012), "Digital Watermarking: Review",[11] In this paper, the DCT algorithm is selected to do the application test of digital image copyright protection. The experiment proves that DCT-based watermark can well withstand a variety of image processing, and the watermark can survive after compression, cropping, and other attacks. The two dimension discrete cosine transform is encoded on the Windows platform by using Visual C++ program language. The experiment result shows that the digital watermark is non-perceptible; the watermark information can be extracted even if it has been attacked and the expected effect can be achieved.

H. K.Ganesan and Tarun Kumar Guptha(2010), "Multiple Binary Images Watermarking in Spatial and Frequency Domains"[7] In this paper, watermarking scheme provides 24 binary images to be embedded in the frequency domain and also 12 more binary images in the spatial domain. The capacity of the watermark to be embedded in the host image is much greater. Therefore, not only the size of watermark increases, but also it ensures acceptable level of security and imperceptibility. Hence, by using the combinational scheme 36 images in total can be embedded in a single RGB image.

I. Jeng-Shyang Pan, Hao Luo, and Zhe-Ming Lu(2006), "A Lossless Watermarking Scheme for Halftone Image Authentication"[8] . Authentication watermark is a hidden data inserted into an image that can be applied to detect any unauthorized change of the image. Here a block-based method is used. In this, 512×512 halftone images are selected to test the effectiveness of the method. The halftone image is divided into 4×4 blocks. The original watermark, i.e. the hash sequence of image, is computed by the MD5 hash function. After translating the string into "0-1" sequence, 128-bit digest is obtained. In authentication, the watermark is extracted from the watermarked image, and the hash sequence is computed from the restored image. When the two sequences are equal, it is confirmed that the watermarked image has suffered no alteration. Both of them are equal to the original watermark.

J. Ali Al-Haj(2007), "Combined DWT-DCT Digital Image Watermarking"[9] In this paper, Watermarking is done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improves the watermarking performance considerably when it is compared to the DWT-Only watermarking approach.

K. Ms. Pradnya, B. Rane and Dr.B.B.Meshram, "XML-Based Security for E-commerce Application". [10] In this paper, they propose XML watermarking in combination with digital signature for security concerns for payment details of the customers. E-commerce based XML data can be easily captured and tempered as it is presented in plain text. Unlike multimedia data, XML data are diverse in nature where watermarking must be invisible and robust. For watermarking SHA- 512 algorithm is used to get hash of transactional data or payment detail (XML file). First, read XML file, partition XML data. Then this Hash value is embedded in the bit positions of XML file. Then digital signature of watermarked XML is computed. For calculating digital signature of watermarked XML data, they have used SHA1 with DSA algorithm.

To measure the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used. A glance on the following table reveals the performance and effectiveness of above mentioned research work. The mentioned PSNR values are also given for a comparative analysis.

Application	Algorithm	Performance
Online Secure ID card Authentication, Online passport Authentication System on Ecommerce model [3]	A Block based algorithm using Hadamard Pattern in spatial domain.	Accuracy is of 99% in average to achieve high quality watermarked images. PS distortion model of halftone effect (variable for scanners and printers) is not required. PSNR ratio is approx. 43 DB
Watermarking Technique applied in a QR code image [2]	Robust Invisible QR Code Image Watermarking Algorithm in SWT Domain (frequency domain)	A novel method to embed the QR code into digital images, lowering the JPEG degradation. It can achieve viable copyright protection and authentication. Most robust to attacks in different considerations. PSNR ratio on various images is approx. 47 DB
Colour Image Watermarking encrypted in QR code [4]	XOR operation for encryption of QR code and watermark, after applying DWT on the Cover image	This algorithm is robust and enhances the security. It does not change the quality of watermarked image. Simple XOR operation is used for encryption. PSNR ratio on various images is approx. 62 DB
Digital Image Watermarking for compressed image format (such as JPEG format) used on the web [5]	Robust and Invisible digital image watermarking algorithm through a 2D barcode and scrambling method based on DWT DFRNT transform. The Watermark extraction process is the inverse of watermark embedding process.	PSNR ratio is approx. 40 DB for various images.
Authentication of Medical Images [6]	Elliptic Curve Cryptography (ECC) algorithm, along with LSB data embedding and through Lossless Watermarking (LWM) Technique.	Lossless Watermarking Image Authentication with high embedding capacity with complete recovery of original images. PSNR ratio is approx. 73 DB for various images.

Digital watermarking for images Copyright Protection, Broadcast Monitoring, Content Authentication, Copy and Playback Control etc. [11]	DCT algorithm for multimedia information Security protection, encoded in Windows platform using visual C++ program.	DCT-based watermark can well withstand a variety of image processing, and it can survive after attacks like compression, cropping etc.
Multiple Binary Images Watermarking in Spatial and Frequency Domains [7]	In frequency domain, DCT is applied to each component of the host image and the watermarked image. For spatial domain LSB bits of the pixel values of the host image are changed.	More data can be inserted into an image and extra level of security is achieved by scrambling image before embedding into the host image. For obtaining better result maximum of 30 binary images can be embedded in a single RGB host image. The PSNR values in the DCT domain for each component after applying the corresponding attack on the mark image are ranging between 31 to 51 DB. This scheme is robust against Gaussian noise and JPEG compression up to 90%. The major advantage is the increase in the capacity with less distortion.
Authentication of Military maps, great works of art, medical images etc. using Lossless Watermarking Scheme for Halftone Images [8]	Digital Halftoning on multi-toning images with hash sequence of original image with MD5 hash function.	Fragile watermarking with low quality distortion is introduced to the halftone images. Original image can be perfectly recovered by reverse process of watermarking application. Only secret key is to be saved.
Combined DWT-DCT Digital Image Watermarking [9]	A combined DWT-DCT (Discrete Wavelet Transform and the Discrete Cosine Transform) digital image watermarking algorithm.	Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that were based solely on the DWT transform. Imperceptibility performance was better and the robustness got improved. PSNR for different sub-bands (HL2 HH2) is approx. 97 DB.
Watermarking Technique for payment database security and XML data security [10]	Digital Signature based SHA1 with DSA algorithm	It shows good result for integrity and authentication of data centric, numeric or document centric, verbose XML data. Even after hijacking digital signature, the hackers get watermarked XML data which is unreadable format for humans.

III. CONCLUSION

In this paper, a brief investigation of several works in past decades on digital watermarking (literature review) is done to overview the development of Digital Watermarking Techniques. The encrypted digital watermarking can not only be used for data authentication but also for secured data transmission. The entrusted algorithms with little modification can be used in various fields starting from media industry to medical science and even for e-commerce transaction. The application area of digital watermarking is very wide. And new novel approaches can be sought. The information provided in this paper on this area may help the new researchers to gather knowledge in this domain. Furthermore, researchers can even improve the existing techniques to make them more effective in various novel applications.

REFERENCES

[1] Neil F. Johnson, Zoran Duric, and Sushil Jajodia. "A Role for Digital Watermarking in Electronic Commerce", http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.449.6184&rep=rep1&type=pdf

[2] Swathi.K, Ramudu.K," Robust Invisible QR Code Image Watermarking Algorithm in SWT Domain", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 4, September 2014

[3] Peyman Rahmati, and Andy Adler, and Thomas Tran. "Watermarking in E-commerce", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013

[4] Vinita Gupta, Atul Barve, "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes", International Journal of Computer Applications (0975 – 8887)Volume 100 – No.14, August 2014

[5] M. Kim, D. Li, and S. Hong, "A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents" :Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, 2013, San Francisco, USA

[6] Arathi Chitla, M. Chandra Mohan," Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)", International Journal of Computer Applications (0975 – 8887) Volume 57– No.6, November 2012

[7] K.Ganesan and Tarun Kumar Guptha, "Multiple Binary Images Watermarking in Spatial and Frequency Domains, Signal & Image Processing" : An International Journal(SIPIJ) Vol.1, No.2, December 2010

[8] Jeng-Shyang Pan, Hao Luo, and Zhe-Ming Lu, "A Lossless Watermarking Scheme for Halftone Image Authentication", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006

[9] Ali Al-Haj,"Combined DWT-DCT Digital Image Watermarking",Journal of Computer Science 3 (9): 740-746, 2007.

[10] Ms. Pradnya B. Rane, Dr.B.B.Meshram. "Xml-Based Security for E-commerce Application", International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012 1 ISSN 2250-3153

[11] Shraddha S. Katariya. "Digital Watermarking: Review", International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 2, February 2012, ISSN: 2277-3754

[12] http://www.tafinn.com/andyfinnus/Writing/Technology/digital_watermarks.htm

[13] http://www.alpvision.com/watermarking.htm