A Survey & Applications of Various Watermarking & Encryption Techniques

Rahul Kumar Nayak, Prof. Amit Saxena. Dr. Manish Manoria

Abstract— Here the paper contains various watermarking technique implemented so far and their different request areas are analyzed and discussed here. Although various techniques of watermarking are already implemented for the confidential information hiding some of them are examined and collate here on the basis of certain parameters including PNSR, watermark signal strength and Bit Error Rate. Since Watermarking enables hiding of secrete statistics such that the data can be secreting when sending to receiver.

Index Terms— Stegnography, DCT, DWT, Encryption, Digital Signatures, Checksum, LSB.

1 INTRODUCTION

Watermarking is a expertise of hiding secrete information such that the secrete information can't be shared with attacker. It includes low level bit data that marks the information per-copy based or per-provider based. There are various application area where watermarking is efficient used.

Applications [1]

a. Copyright Protection
   i. Content owner embeds a secrete watermark
   ii. Proof of possession by disclosing the secrete key
b. Fingerprinting
   i. Embed a serial number describing the recipient
   ii. Later we can detect which user copied the image.
c. Authentication
d. Integrity Verification
   i. In fragile based watermark guarantee integrity
e. Content labeling
f. Rights Management
   i. Galaxy group
   ii. Contains Secure and Digital Music Initiative
   iii. Inter trust
g. Content Protection.

Information hiding is the ability which provides two sort of information to be shared between users one is steganography and other is watermarking [2, 3], hence on the basis information hiding can be categorised as follows:

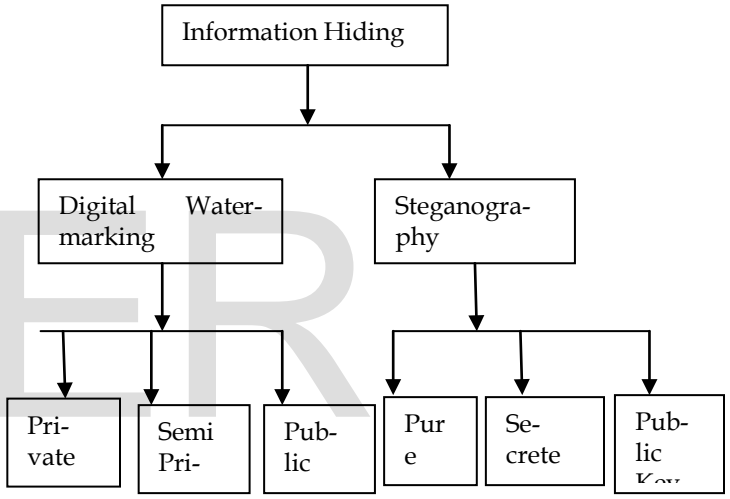

Figure 1. Classification of Information Hiding

Figure 3 shown below is the differentiation of various secretes communication technique used for the secure communication between sender and receiver [4].

	Confidentiability	Integrity	Unremovability
Encryption	YES	NO	YES
Digital Signatures	NO	YES	NO
Steganography	YES/NO	YES/NO	YES

Table1. Comparison o Secrete Information Techniques

Steganography vs watermarking

Although both of the above techniques are based on the same working areas and principles but there occus little difference between two. But both of the method is used for the information hiding [5], [6], [7].

The techniques are used to hide huge amount of information hiding and protection of these data [8].

Figure 2. (a) Original Lena Image (b) The original Facial Women Image (c) The original Moon Image

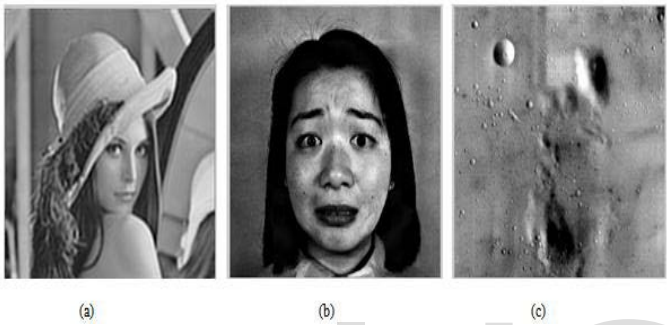

Figure 3. (a) The watermarked image of Lena (b) The Facial watermarked Image (c) Watermarked image of Moon.

Diverse Techniques included in Digital Watermarking

Digital watermarking is a procedure where random information is encoded or hide in image so that the unrevealed material is not visible to the attacker [9]. It can be classified and categorized as spatial domain and frequency domain [10].

Spatial Domain Techniques

In this method, the watermark is inserted in the wrap image altering pixels or image individuality [11]. The algorithm should cautiously consider the numeral of distorted bits in the pixels against the probability of the watermark becoming visible [12]. Mahfuzur Rahman and Koichi Harada suggested a method to lodge in order in objects with layered 3D triangular meshes of a kind that those reconstructed from CT or MI data, a parity intensify topology based spot area watermarking method [9].

Frequency Domain Techniques

With compared to the spatial domain techniques frequency domain technique is more useful and applied mostly. The most repeatedly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The (DWT) and the (DCT) are implemented very effectively in numerous digital images watermarking scheme. In this new age Singular Value Decomposition (SVD) is also implementing very efficiently in the digital image watermarking scheme.

Embedding check-sums in LSB

One of the first approach used for image tampering detection was based on inserting check-sums into the least significant bits (LSB) of the image data. The algorithm was proposed by Walton [13] in the year 1995 consists in selecting, according to a secret key, pseudorandom groups of pixels. The check-sum value is obtained by the summation of the numbers determined by the 7 most significant bits (MSB) of the selected pixels. Then the check-sum bits are implanted in the LSB. The basic version of this algorithm can be summarized as:

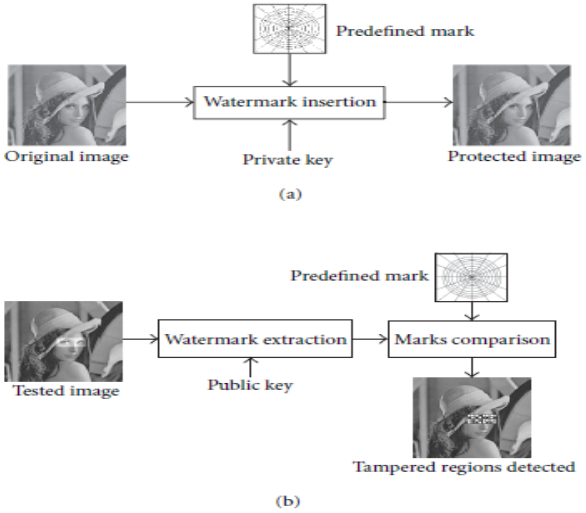

Figure 4: Generic fragile watermark scheme: (a) Image security. (b) Authenticity verification.

2 Literature Survey

Manjit Thapa, Dr. sandeep kumar sood and A.P. meenakshi Sharma proposed a new and efficient technique of watermarking based on varied types of stormings [14]. In this paper an efficient watermarking deployed on singular value decomposition is proposed which provides efficient results as compared to the other existing technique implemented for watermarking. The technique efficient detects and extract untold information from the image without any error rate. The technique strongly resist against various attacks.

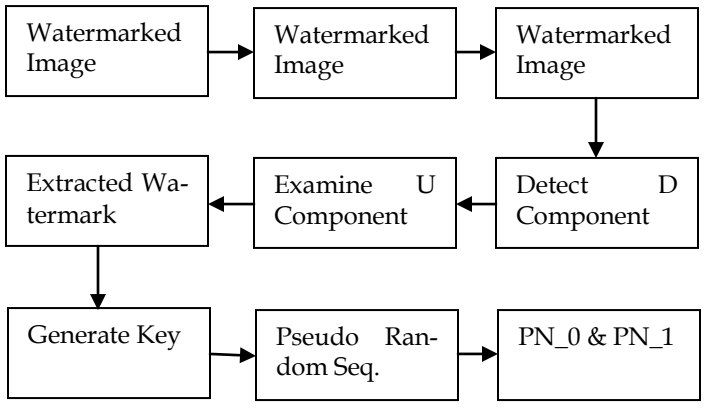

Figure 5. Watermark Extraction Algorithm [1]

In the following paper, one propose a robust watermark embedding technique for JPEG2000 compressed and encrypted

images. While the proposed technique embeds watermark in the compressed encrypted domain, the watermark can be extraced either in decrypted domain or in encrypted domain and found out a technique to embed a robust watermark in the JPEG2000 compressed encrypted images. The algorithm is easier to implement as it is directly performed on the compressed-encrypted domain i.e it does not require decryption or partial decompression of the contents [15].

In 2012 by Anamitra Makur, Nikhil Narayan S. "Tamper-Proof Image Watermarking using Self-Embedding". Here propose a breakable watermarking with self-embedding for retrieval of tampered image that does not use authentication bits. We use a robust spread spectrum based watermarking scheme using block based embedding, DCT based compression, and other upgrades.Simulation results showing recovery performance are presented and find out the Conclusion we develop a novel algorithm for tamper detection and recovery of images using no authentication bit and robust watermarking [16].

Here, the watermark is used not only for tamper detection, but it also contains enough information relating the cover image and thus help in recovering the tampered parts of the received image. We have used a DCT based image compression scheme, spread spectrum image steganography so as to embed the watermark, many error correction schemes (both at the encoder and decoder) to enhance the watermark extraction, and cautious selection of global and local MSE threshold, to achieve up to ninety percent restoration of the tampered images[16].

While the traditional approach of encrypting enhancement layers experience high computational encryption demand and disadvantages in distribution, the proposed window encryption approach can cut price of computational and permits a controlled modification of the required security for many requisition scenarios and results in Conclusion In this work have proposed the window encryption perspective for efficient transparent encryption with JPEG2000. The application of JPEG 2000 error concealment strategies to facilitate the effective deployment of clear JPEG2000 encryption is proposed and experimentally approved [17].

In 1999 by Saraju Prasad Mohanty gives the concept about Watermarking is the procedure of fixing data called a watermark (also known as Digital Signature or Tag or Label) into a multimedia object such that watermark can be identified or withdraw later to make an assertion about the object. The object may be an audio, image or video. An easier example of digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the object. Based on the purpose of the watermark, it is embedded either visibly or invisibly.

In 2010 by A. V. Subramanyam , Sabu Emmanuel, Mohan S. Kankanhalli [18] proposed an improved way of embedding the watermarking either by first applying the compression or encryption and is performed on jpeg2000 image. The techniques provide detection of the watermarking at the time of the compression or encryption of the image. The technique is simpler to implement and is efficient as per security is concerned. The technique uses jpeg2000 compression algorithm for the compression of image and stream cipher using RC4 is used for the encryption of the image and the watermark signal generation and detection is done by using spread spectrum technique.

In 2012 by Anamitra Makur, Nikhil Narayan S. [19] proposes a watermarking technique including DCT based compression as an application for the image tempering. The technique uses spread spectrum based watermarking technique which is a brittle watermarking technique. The idea is to detect tamper and provides recovery of images where we do not require authentication bits.

In 2009 by Shiraz Ahmad [20] "Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants" proposed a new robust technique for the watermark images that may be attacked using some geometric transformation of image such as scalling or rotation. The watermarked embedding can be easily detection by transformation of image. Hence proposes a technique to prevent from such attacks by using scale invariant feature transform based bounding boxes and moment-invariant for the watermark embedding which can prevent from geometric attacks.

In 2012, a water mark technique is proposed which is used to retriev tampered documents [21]. The technique is used for the retrieval of the documents using pixel flipping and then self-embedding so that the authentication is achieved. This technique recovers against all sort of attacks possible in tampered document such as insertion or substitution or deletion.

In 2012, Soumya Mukherjee, Arup Kumar Pal proposed a newer technique of water marking using the combinatorial method of discrete wavelet transform and singular value decomposition on gray scale images. The technique implemented here for watermarking is suitable to prevent the gray images from various attacks such as nosing, cropping or image enhancement [22].

In 2012, digital video watermarking has been sugested [23]. Although there many watermarking techniques implemented for the video, here a new technique has been implemented where the video is first divide into a number of frames and a key is used which is applied on each frame for the encryption of the frames and the same key is then applied for the decryption of video frames and the frames are then arranged to get the original video in a secure way.

In 2012, a digital image watermarking technique has been implemented [24] in which one quad tree based approach is used to select the region of interest (ROI) and then to use the properties of the singular value decomposition (SVD) transform to hidde of the watermark is being put forward here.

In 2012, a blind watermarking technique has been lodged using the concept of DCT [25]. Here the watermarking using DCT can be given by evaluating correlated coefficient between the extracted coefficients of the watermarked image and then the partial watermark values that are known are calculated.

Algorithm	Advantages	Disadvantages
LSB	1. Easier to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Correlation	1. Gain factor can be Enhanced resulting in increased ability to cope with errors during execution.	1. Image quality gets Decreased due to very high increase in gain factor.
PatchWork	1. High level of robustness against most type of attacks	1. It can hide only a very fewer amount of information.
Texture mapping coding	1. This method hides data within the continuous random texture patterns of a picture.	1. This algorithm is only suitable for those areas with huge number of arbitrary texture images.
DCT	1. The watermark is inserted into the coefficients of the middle frequency, so the visibility of image should not get affected and the watermark will not be recovered or removed by any kind of attack.	1. Block wise DCT demolish the invariance properties of the system. 2. Certain higher frequency components tend to be subdue during the quantization step.
DWT	1. Allows advantageous localization both in time and spatial frequency domain 2. More compression ratio which is relevant to human perception.	1. Computational cost may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Price of computing may be higher.
SS	1. Efficient to implement and strength of watermarking is more.	1. Requires more computation time.
Scalar Costa Scheme Quantization Index Modulation	1. Distortion level is less and more PSNR.	1. More BER.

Table 2. Comparison of Watermarking Techniques

Algorithm	Structure	Key Size (bits)	Rounds	Cipher Type
AES	Substitution-permutation network	128, 192, 256	10, 12, 14	Block
DES	Balanced Feistel network	56	16	Block
T-DES	Feistel network	112, 168	48	Block
RC2	Source-heavy Feistel network	40 to 1024	18	Block
Blowfish	Feistel network	32 to 448	16	Block
Skipjack	Unbalanced Feistel network	80	32	Block
RC4	-	40 to 2048	256	Stream

Table 3. Comparison of Various Encryption Techniques

REFERENCES

[1] Doug Tygar, "Watermarking", Available at https://inst.eecs.berkeley.edu/~cs161/fa05/Notes/cs161.1130.pdf.

[2] A.A.Zaidan, Fazidah. Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography ", World Congress on Engineering 2009 (WCE), The 2009 International Conference of Computer Science and Engineering, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009, ISBN: 978-988-17012-5-1, Vol.I, p.p259-265.

[3] A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B. Zaidan, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session 9, P.P 425 429.

[4] R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and JOURNAL OF COMPUTING, VOLUME 2, ISSUE 2, FEBRUARY 2010, ISSN 2151-9617 https://sites.google.com/site/journalofcomuting/ Computers, Department of Computer Science and Software Engineering.

[5] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "New Approach of Hidden Data in the portable Executable File without Change the Size of Carrier File Using Distortion Techniques", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 493-497.

[6] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502.

[7] M. Abomhara, Omar Zakaria, Othman O. Khalifa , A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore.

[8] Md. Rafiqul Islam, A.W. Naji, A.A.Zaidan, B.B.Zaidan " New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques", International Journal of Computer Science and Information Security (IJCSIS), ISSN: 1947-5500, P.P 273-279, Vol.7 , NO.1, January 2010, USA.

[9] Md. Mahfuzur Rahman and Koichi Harada, "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", IJCHNS International Journal of Computer Science and Network Security, Vol. 6, No. 2A, February 2006.

[10] M. Hamad Hassan, and A.A.M.Gilani, "A Fragile Watermarking Scheme for Color Image Authentication", International Journal of Applied Science, Engineering and Technology, Vol. 1, No. 3, pp.-156-160, 2005.

[11] M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain", University of Bonn Germany, Tech. Rep., 2006.

[12] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection, Artech House, 2003.

[13] S. Walton, "Information authentification for a slippery new age," Dr. Dobbs Journal, vol. 20, no. 4, pp. 18–26, 1995.

[14] Manit Thapa, Dr. Sandeep Kumar sood, A.P. meenakshi Sharma," Digital Image Watermarking", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011.

[15] A. V. Subramanyam, Sabu Emmanuel, Mohan S. Kankanhalli, "compressed-encrypted domain jpeg2000 image watermarking." School of Computer Engineering, Nanyang Technological University, Singapore School of Computing, National University of Singapore, Singapore, 978-1-4244-7493-6/10/$26.00c IEEE 2010 .

[16] Anamitra Makur, Nikhil Narayan S. "Tamper-Proof Image Watermarking using Self-Embedding" Electrical & Electronic Nanyang Technological University, Singapore, acm-2012.

[17] Thomas Stütz and Andreas Uhl " On Efficient Transparent JPEG2000 Encryption" Dept. of Computer Sciences, University of Salzburg Salzburg, Austria,acm-2007.

[18] A. V. Subramanyam, Sabu Emmanuel, Mohan S. Kankanhalli, "compressed-encrypted domain jpeg2000 image watermarking." School of Computer Engineering, Nanyang Technological University, Singapore School of Computing, National University of Singapore, Singapore, 978-1-4244-7493-6/10/$26.00□c 2010 IEEE.

[19] Anamitra Makur, Nikhil Narayan S. "Tamper-Proof Image Watermarking using Self-Embedding" Electrical & Electronic Nanyang Technological University, Singapore,acm-2012.

[20] Shiraz Ahmad "Feature-based Watermarking using Discrete Orthogonal Hahn Moment Invariants" Proceedings of the 7th International Conference on Frontiers of Information Technology (FIT-09), Article No. 38, 2009.

[21] Anamitra Makur, Govindarajan Sridharan," Watermark based Recovery of Tampered Documents",ACM 2012.

[22] Soumya Mukherjee, Arup Kumar Pal," A DCT-SVD based Robust Watermarking Scheme for Grayscale Image", ACM 2012.

[23] Ujan Mukhopadhyay, Souptik Sinha, Poulomi Ghosh, Rilok Ghosh, Dipak kr. Kole and Aruna Chakroborty," Enhancing the Security of Digital Video Watermarking using Watermark Encryption",ACM 2012.

[24] Priyanka Singh, Suneeta Agarwal," A Region Specific Robust Watermarking Scheme Based on Singular Value Decomposition",ACM 2012.

[25] Reena Gunjan, Vijay Laxmi, Manoj S. Gaur," Detection Attack Analysis using Partial Watermark in DCT Domain", ACM 2012.