Volume 2, Issue 1, January 2015 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

An Approach for Information Hiding Using Various Watermarking Techniques-A Survey

Prashasti Chaturvedi
M.Tech. Research Scholar
Department of Computer Science Engineering
Jai Narain College of Technology (JNCT)
Bhopal (M.P.) [INDIA]
Email : pprashastichaturvedi@gmail.com

Prof. Raghvendra Singh Tomar
Assistant Professor
Department of Computer Science Engineering
Jai Narain College of Technology (JNCT)
Bhopal (M.P.) [INDIA]
Email: raghvendra01@gmail.com

Prof. Sweta Gupta
Assistant Professor
Department of Computer Science Engineering
SISTEC-E
Bhopal (M.P.) [INDIA]
Email: 6.swetagupta@gmail.com

Dr. Mukta Bhatele
Professor & Head of the Department
Department of Computer Science Engineering
Jai Narain College of Technology (JNCT)
Bhopal (M.P.) [INDIA]
Email: mukta_bhatele@rediffmail.com

ABSTRACT

Here in this *paper various watermarking technique implemented so far and their different application areas are discussed and analyzed. Although there are various watermarking techniques implemented for the secrete information hiding some of them are analyzed and compared here on the basis of certain parameters such as PNSR, watermark signal strength and Bit Error Rate. Since Watermarking enables hiding of secrete information such that the information can be secreting when sending to receiver.*

Keywords:— *Steganography, DCT, DWT, Encryption, Digital Signatures, Check Sum, LSB.*

I. INTRODUCTION

Watermarking is a technique 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 ownership 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. A fragile watermark assures integrity
e. Content labeling
f. Rights Management
   i. Galaxy group
   ii. Secure Digital Music Initiative
   Iii. Interrupt
g. Content Protection.

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

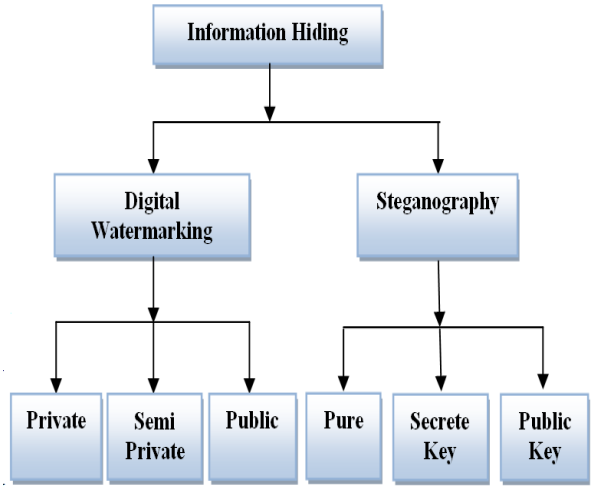

Figure 2. Classification of Information Hiding

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

	Confidenti-ability	Integ-rity	Unremov-ability
Encryption	YES	NO	YES
Digital Signatures	NO	YES	NO
Steganogr-phy	YES/NO	YES/ NO	YES

Figure 3. 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 is a little difference between two. But both of the technique is used for the information hiding [5], [6], [7].

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

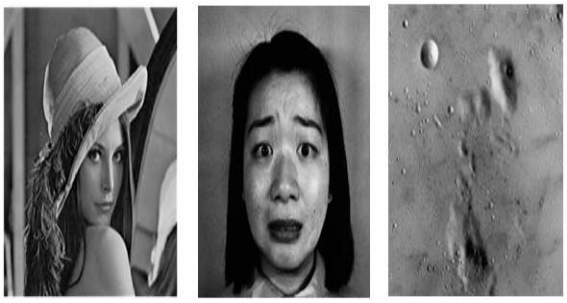

Figure 4. Three original images of 256 × 256 pixels (a) The original Lena Image (b) The original Facial Image (c) The original Moon Image

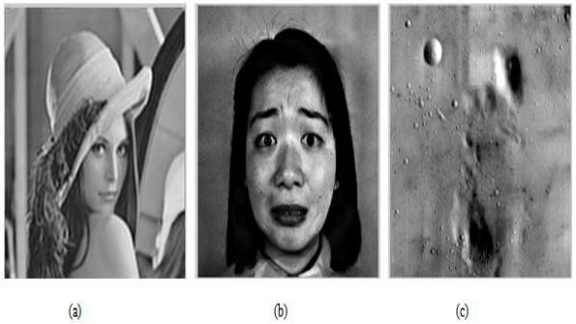

Figure 5.Three watermarked images of 256×256 pixels (a) The watermarked Lena Image (b) The watermarked Facial Image (c) The watermarked Moon Image.

Different Techniques of Digital Watermarking

Digital watermarking is a process where arbitrary information is encoded or hide in image so that the secrete information 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 technique, the watermark is inserted in the cover image changing pixels or image characteristics[11]. The algorithm should carefully weigh the number of changed bits in the pixels against the possibility of the watermark becoming visible[12]. Mahfuzur Rahman and Koichi Harada proposed a method to insert information in objects with layered 3D triangular meshes such as those reconstructed from CT or MI data, a parity enhanced 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 commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The discrete wavelet transforms (DWT) and the discrete cosine transforms (DCT) are implemented very effectively in numerous digital images watermarking scheme. In this new era Singular Value Decomposition (SVD) is also implementing very effectively in the digital image watermarking scheme.

Embedding check-sums in LSB

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

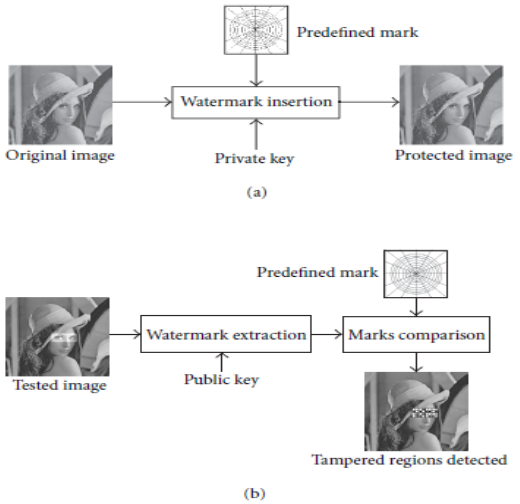

Figure 6: Generic fragile watermark scheme: (a) Image security. (b) Authenticity verification.

II. LITERATURE SURVEY

Manjit Thapa, Dr. Sandeep Kumar sood and A.P. meenakshi Sharma proposed a new and efficient technique of watermarking based on various types of attacks [14]. In this paper an efficient watermarking based 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 secrete information from the image without any error rate. The technique strongly resist against various attacks.

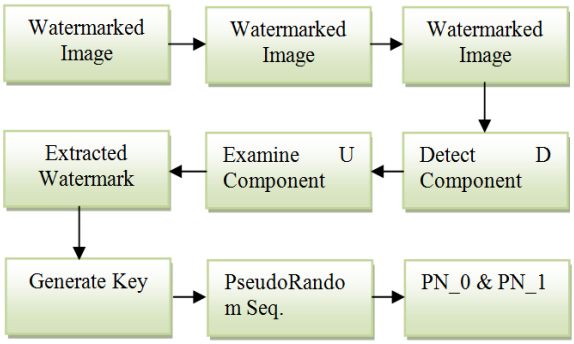

Figure 7. Watermark Extraction Algorithm [1]

In this paper, we propose a robust watermark embedding technique for JPEG2000 compressed and encrypted images. While the proposed technique embeds watermark in the compressed encrypted domain, the extraction of watermark can be done either in decrypted domain or in encrypted domain and found out the Conclusion a technique to embed a robust watermark in the JPEG2000 compressed encrypted images. The algorithm is simple to implement as it is directly performed on the compressed-encrypted domain i.e it does not require decrypting or partial decompression of the content [15].

In 2012 by Anamitra Makur, Nikhil Narayan S. “Tamper-Proof Image Watermarking using Self-Embedding”. Here propose a fragile watermarking with self-embedding for recovery 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 improvements. 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 not only used for tamper detection, but it also carries enough information regarding the cover image so as to help in recovering the tampered parts of the received image. We have used a DCT based image compression scheme, spread spectrum image steganography to embed the watermark, several error correction schemes (both at the encoder and decoder) to enhance the watermark extraction, and careful selection of global and local MSE thresholds, to achieve up to 90% restoration of the tampered image[16].

While the traditional approach of encrypting enhancement layers suffers from high computational encryption demand and drawbacks in distribution, the proposed window encryption approach can reduce computational cost and allows a controlled adaptation of the required security for many application scenarios and find out the Conclusion In this work have proposed the window encryption approach for efficient transparent encryption with JPEG2000. The application of JPEG2000 error concealment strategies to facilitate the effective deployment of transparent JPEG2000 encryption is proposed and experimentally approved[17].

In 1999 by Saraju Prasad Mohanty gives the concept about Watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an audio, image or video. A simple 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.

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.

* * * * *