International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

# A REVIEW ARTICLE OF WATERMARKING

**Mandeep Kaur[(1)] , Navneet Kaur[(2)] ,Chetan Batra[(3)]**

**[(1)]Lecturer in Shaheed Bhagat Singh State Technical Campus(Poly), Ferozepur**

**menuk8@gmail.com**

**[(2)]Research Scholar**

**navneet18kaur@gmail.com**

**[(3)]Lecturer in Shaheed Bhagat Singh State Technical Campus (Poly), Ferozepur**

**chetan.batra55@gmail.com**

## ABSTRACT

In most of the digital image watermarking schemes, it becomes a common practice to address *security* in terms of *robustness*, which is basically a norm in cryptography. Such consideration in developing and evaluation of a watermarking scheme may severely affect the performance and render the scheme ultimately unusable. Watermarking is the process of embedding watermark into an image such that the embedded watermark can be extracted later. Lossy compression attacks in digital watermarking are one of the major issues in digital watermarking. Cheddad et al. proposed a robust secured self-embedding method which is resistant to a certain amount of JPEG compression. Our experimental results show that the self-embedding method is resistant to JPEG compression attacks and not resistant to other lossy compression attacks such as Block Truncation Coding (BTC) and Singular Value Decomposition (SVD). Therefore we improved Cheddad at all's. Method to give better protection against BTC and SVD compression attacks.

## KEYWORDS

Image watermarking; Robustness; Security

## INTRODUCTION

Today, many photo agencies expose their collection on the web with a view of selling access to the images. They typically create web pages of thumbnails, from which it is possible to purchase high resolution images. However, this kind of ultimate flexibility to avail digital images facilitates information piracy. Cryptographic techniques can solve the problem of unauthorized access to the information. But, it can't prevent an authorized user from illegally replicating the decrypted content. Watermarking schemes in their early days, building on the steganography or information hiding concept, were assumed to be secure if a watermark could not be seen (i.e., hidden) and could not be removed from audio-visual objects by common processing tools [1]. In digital image watermarking, the essence of such an assumption lies in two corrections: i) hiding the watermark in the cover image imperceptibly, and ii) its robustness to any kind of transforms. Addressing these two criteria in terms of fidelity (or imperceptibility) and robustness has become a common practice in digital image watermarking research, where it is assumed that they would satisfy the necessary security requirements. Thus, improving robustness with an acceptable fidelity underpins several watermarking Schemes, for example [2-4]. In some application scenarios, this may be still valid, where there are no strict security requirements. However, the big-assumption – just mentioned, does not satisfy various security requirements of digital image watermarking in a number of applications. For example, copyright protection, content authentication, integrity control, and transaction tracking are some that gained much attention recently in the field. Each target application imposes different requirements in watermarking that result in variations in the underlying algorithms. These variations are often expected, although an inadequate assessment to those variations in requirements of different watermarking parameters aiming at a particular scenario can severely affect the watermarking performance. A good example in this context is robustness and security that we are particularly interested in and limit our attention to in this paper. The content of watermarked digital images can be easily attacked by using image processing operations such as lossy compression. Invisible watermarking requires a reasonable robustness against compression attacks. Lossy compression algorithms tend to remove invisible information that can be related to the watermark. Watermark robustness under image compression is an essential issue for image content protection. Therefore, watermarks should combine invisibility and robustness simultaneously. Recently Cheddad et al [6] proposed a method to protect the digital image itself using a secured robust self embedding technique. In their method, a halftoned version (black and white image) of the original image is used as watermark. The calculated watermark is embedded in the 2D Haar DWT of the original image and the watermarked image is obtained. Then the Wavelet-based Inverse Half toning via De-convolution (WInHD) is used on the extracted watermark from the watermarked image to recover the approximation of the original image. This is a blind watermarking scheme as the original image is not needed for the recovery process, see Figure 1.

International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

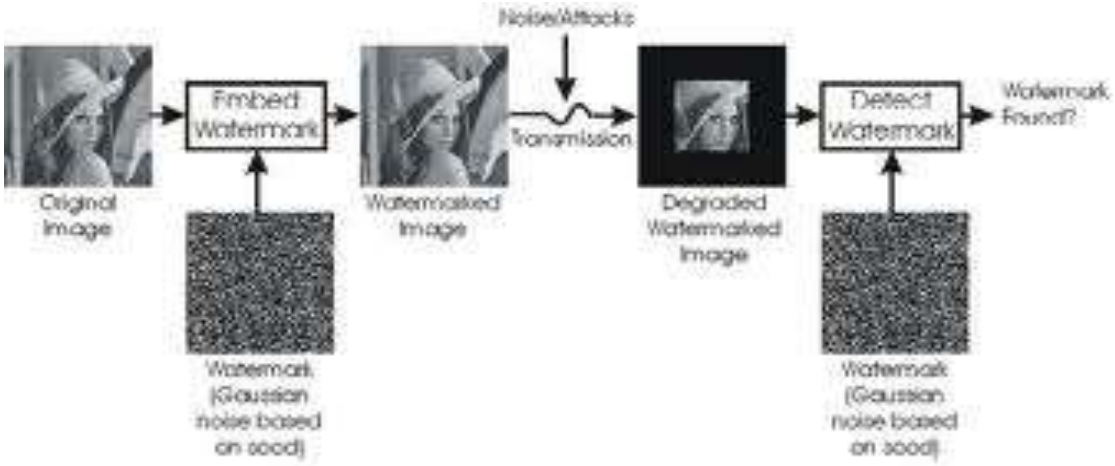


**Fig-1**

JPEG 2000 is one of the modern lossy compression methods and it is based on DWT. As the Cheddad et al. method is DWT based; it is resistant to JPEG compression attacks to a certain extent. They reported that their method is resilient to JPEG compression up to 80-75% [6]. There are no experimental results shown for other lossy compression techniques, such as Block Truncation Coding (BLC) and Singular Value Decomposition (SVD) etc. Our experimental results show that Cheddad at all's method is not robust to BTC and SVD lossy compression techniques. Therefore we improved Cheddad at all's method and experimental results prove that our method provides better recovery results on BTC and SVD compression attacks.

## Verifying Integrity of medical image with lossless watermarking

Integrity control of images can be addressed at two levels, that is: strict integrity control whereby one has to guarantee that the whole image is preserved as entire bit planes, or; content-based control in which pixels are allowed to vary while the visual content meaning remains preserved. In this work our interest is given to strict integrity which can be achieved by making use of cryptographic hash function. Cryptographic hash functions are commonly used for digital signatures as they extract a resume or digest from the message data to be protected. Between the two function classes, the first one, called Message Code Authentica-tion (MCA), uses a secret key and permits signature identification. The second one, known as Manipulation Detection Code (MDC), is calculated without a secret key. Since MCA function usually makes use of a MDC function concatenated with a secret key or asymmetrically encrypted, interest is given here to MDC hash function. These functions are said one way hash functions (i.e. non reversible), and from a message of arbitrary length they provide a fixed length digest or resume. For example, one of the best known methods is the SHA-256 (Secure Hash Algorithm) that yields to a signature of 256 bits [6]. Its collision probability, that is the probability to and another message with the same hash, is upper bounded by 1=2256. SHA also has good dispersion property in that a slight deference in a message will lead to a very die rent signature. Such a cryptographic hash can be encrypted in asymmetric way allowing non repudiation property. The RSA (Rivest Shamir Adleman) algorithm [7] is the most widely-used asymmetric system. The system uses two deferent keys for encryption and decryption. One of these two keys, the public key, is meant to be known to everyone, and the other, the private key, is known to only one individual. In order to write to a recipient, all that needs to happen is to encrypt the message with the public key of the recipient. Upon reception, only the recipient will be able to decrypt the message with his private key. Data congeniality is ensured in that case. The RSA algorithm allows also encryption with one's own private key (signature). In this case, everyone can read the message thanks to the public key. Since the sender is potentially the only person who could have encrypted it with his private key: the sender has signed the message. In DICOM (Digital Imaging and Communications in Medicine), the standard of reference for medical image storage and sharing (medical.nema.org), there exists a digital signature problem based on the RSA. This problem is combined with the RIPEMD-160, MD5, or SHA-1 hashing functions to generate a MAC (Message Authentication Code), which is encrypted using a private RSA key. This digital signature is actually stored in the header of a DICOM image _le. Hal-00447047, version 1 - 14 Jan 20104 reversibly watermarking a cryptographic hash within a medical image leads to the integrity control process illustrated in Fig. 1. A hash of the image I to be protected is calculated making use of a cryptographic hash function H (H(I)) and is then embedded in I leading to the watermarked image Iw. At the variation stage, the watermark reader extracts the hash H (I) and removes the watermark from Iw obtaining the restored image Ir. H (I) is compared to H (Ir). If H (I) and H (Ir) are equal then Ir is said to be identical to I; if not, the system states that the image has been modied. The hash can be calculated on the image pixel gray values or on the full representation of the document. In the latter case the integrity will also depend on the image format.

International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

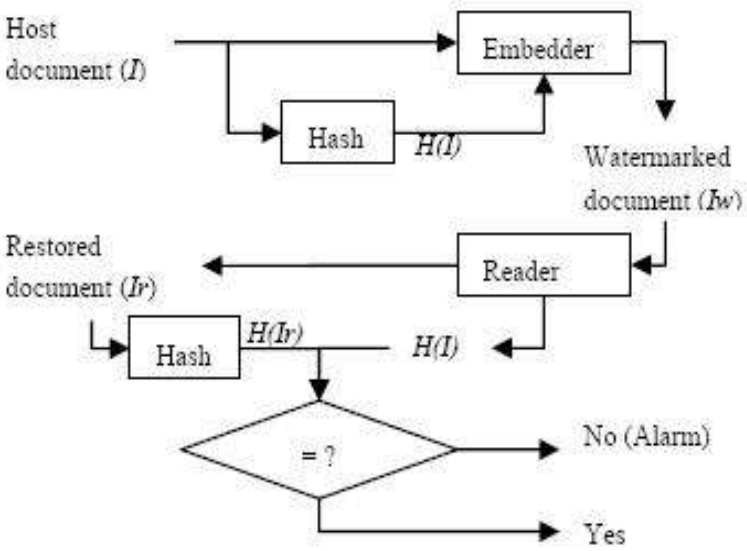


**Fig-2**

## CONCLUSIONS

In this paper, we discussed and analysed a fundamental problem in the realization of watermarking security and robustness. We started with figuring out the problem status in various individual watermarking schemes developed so far. With the help of statistical analysis, we demonstrated the research status and general trends of those two particular directions in watermarking research. The analyses help realize that even having the similar importance, one parameter is receiving more attention than the other. Thus, the lesser attention to the security problems suggests the wrong perception on the watermarking security, which has been continuously influenced by the original assumption we discussed in the beginning of this paper. Moreover, in order to explore how addressing security requirements in terms of achieving robustness leads to an inadequate assessment for a digital image watermarking scheme, we posed a key question in the problem domain. A theoretical analysis is then presented considering respective set of requirements for security against attacks, and robustness to distortions. Thereby, we successfully demonstrated that neither security nor robustness can completely counteract each other. This realization imposes individual and careful considerations for the both parameters, not only in developing a watermarking scheme but also in its assessment to be complete. Finally, we presented some necessary directions to developing a complete framework for evaluating both parameters. We believe the realization, analyses, and directions presented in this paper will promote necessary awareness of robustness and security considerations in both developing and evaluating a watermarking schemes in future research. Since there is no existing general framework appropriate for a complete assessment of the parameters for our future work, we expect to develop such frameworks for the parameters in a digital image application.

## REFERENCES

[1]. L. Liu, D.-C. Lou, M.-C. Chang, and H.-K. Tso, "A robust watermarking scheme using self-reference image," Computer Standards & Interfaces, vol. 28, pp. 356-367, 2006.

[2] D. Simitopoulos, D. E. Koutsonanos, and M. G. Strintzis, "Robust image watermarking based on generalized Radon transformations," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 13, pp. 732-745, 2003.

[3] C. Rey and J. L. Dugelay, "Blind detection of malicious alterations on still images using robust watermarks," in Secure Images and Image Authentication (Ref. No. 2000/039), IEEE Seminar on, 2000, pp. 7/1-7/6.

[4] H. Nyeem, W. Boles, and C. Boyd, "Developing a digital image watermarking model," in Digital Image Computing Techniques and Applications (DICTA), 2011 International Conference on, Noosa, Queensland, Australia, 2011, pp. 468-473.

[5] A. Piper and R. Safavi-Naini, "How to Compare Image Watermarking Algorithms," in Transactions on Data Hiding and Multimedia Security IV. vol. 5510, Y. Shi, Ed., ed: Springer Berlin / Heidelberg, 2009, pp. 1-28.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. ed. Burlington :: Elsevier, 2007.

[7] A. Tefas, N. Nikolaidis, and I. Pitas, "Chapter 22 – Image Watermarking: Techniques and Applications," in The Essential Guide to Image Processing (Second Edition), B. Al, Ed., ed Boston: Academic Press, 2009, pp. 597-648.

[8] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," Communications Magazine, IEEE, vol. 39, pp. 118-126, 2001.

[9] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, pp. 385-403, 1998.

[10] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[11] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," Signal Processing, vol. 87, pp. 1264-1280, 2007.

[12] C. Deng, X. Gao, X. Li, and D. Tao, "A local Tchebichef moments-based robust image watermarking," Signal Processing, vol. 89, pp. 1531-1539, 2009.

[13] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," presented at the Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany, 2004.

[14] F. Y. Shih and Y.-T. Wu, "Robust watermarking and compression for medical images based on genetic algorithms," Information Sciences, vol. 175, pp. 200-216, 2005.

[15] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: theory and practice," Signal Processing, IEEE Transactions on, vol. 53, pp. 3976-3987, 2005.

[16] T. Furon, "A survey of watermarking security," in International Workshop on Digital Watermarking, 2005, pp. 201--215.

[17] Q. Li, N. Memon, and H. T. Sencar, "Security issues in watermarking applications - A deeper look," in ACM International Workshop on Multimedia Contents Protection and Security, MCPS 2006, co-located with the 2006 ACM International Multimedia Conference, October 28, 2007 - October 28, 2007, Santa Barbara, CA, United states, 2006, pp. 23-28.

[18] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol. 10, pp. 1593-1601, 2001.

[19] J. M. Zain and A. R. M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AWTDR)," in Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, 2007, pp. 5661-5664.

[21] S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery," in Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, 2010, pp. 417-420.

[22] S. Braci, R. Boyer, and C. Delpha, "Security evaluation of informed watermarking schemes," in Image Processing (ICIP), 2009 16th IEEE International Conference on, 2009, pp. 117- 120.

[23] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," Signal Processing, vol. 83, pp. 2069-2084, 2003.