

# Realization of Highly Secure Fragile Watermarking Technique for Authentication of Digital Images

<sup>1</sup>Nasir N. Hurrah, <sup>2</sup>Nazir A. Loan, <sup>3</sup>Shabir A. Parah and <sup>4</sup>Javaid A. Sheikh

<sup>1,2</sup>Department of Electronics and Inst. Technology, University of Kashmir, India

<sup>3,4</sup>Department of Electronics and Instrumentation Technology, University of Kashmir, India

E-mail: <sup>1</sup>hnasirg01@gmail.com, <sup>2</sup>nazirloan@gmail.com<sup>3</sup>shabirelr@gmail.com

---

**Abstract**—The easily accessible data sharing networks have attracted millions of people to share their important data at a rapid rate. However, this ease has also attracted numerous attacks on copyright protection and authentication of data. These issues creep in because of the fact that digital data like text, images, audio and video could be easily accessed, copied, manipulated and distributed illegally by the help of highly powerful tools. In such a scenario, there is high demand of the techniques which can safeguard this data transmission through these insecure networks and preserve the Intellectual Property Rights (IPR). Digital image watermarking, which deals with embedding a special data (watermark) in a cover medium is the most viable solution to take care of IPR and content authentication. There exist very few techniques which offer satisfactory forgery detection, imperceptibility, payload and security in combination. Also these techniques are meant to be applicable only for gray scale or color or medical images. The proposed work is different from previous ones in the sense that it aims provide all these features without much complexity and speed issue. The proposed work is a blind fragile digital image watermarking scheme and is applicable to all type of gray-scale/color and medical images. For achieving better subjective and objective quality parameters image blocking and encryption techniques have been used prior to embedding the watermark in the cover image. The proposed work formulates a unique spatial domain based tamper detection algorithm for fragile watermarking techniques. The imperceptibility of more than 50dB and fragility with high error rate of greater than 50% is achieved.

## 1. INTRODUCTION

The world is progressing rapidly through state of art technology and for successful implementation of different operations data is exchanged at a staggering rate. The data in the digital form is exchanged involves medical records, multimedia images, audio and video files [1-5]. This data is exchanged between different modules after several clinical trials and real time data acquisitions through sensors, personal fitness band and implanted devices [6-8]. This data is huge, for example a person can generate health related data equivalent to 300 million books data in a lifetime. Privacy and data integrity are one of the important requirements of a system carrying out data transmission, storage, processing and reception. Even if companies and organizations are taking lot of steps for preserving the privacy of the content, data

breaches are highly prevalent in current scenario. This is because of the insecure channels and availability of strong data processing tools. This has demanded from the researchers to develop state of art techniques to preserve the sensitive information and safeguard intellectual property rights (IPR) [9-12].

For ensuring this data safety different precautionary measures are taken by the designers and researchers. Data integrity and authentication are two major concerns before researchers in order to safeguard exchange of data and preserve the privacy and IPR rights [13-15]. Conventional security measures are somewhat effective for ensuring data security but fail to resist most of commonly data manipulations up to an effective level. Digital watermarking is a technique which hides some secret data in some cover media like image, audio or video to ensure security. This hiding is done in such a way that perceptual quality of the media remains intact. The data hidden in a cover media is called watermark [16-20].

In this paper a fragile watermarking scheme is proposed with high level security for authentication purposes. The security is acquired by encrypting the watermark data before embedding process. A secret key is used for encryption which remains available with only authorized users. The authentication is achieved by embedding this encrypted data in the cover image by modifying the spatial domain values.

## 2. RELATED WORK

In recent years the research on watermarking has risen abruptly due to several breaches in data transmission and security issues related to sharing of sensitive information. The watermarking techniques are generally implemented in two domains; Spatial domain and transform domain [20-22]. In spatial domain the watermark is directly embedded in the original values of the cover image while as in transform domain the watermark is hidden in the coefficients in frequency domain. Watermark is generally implemented in spatial domain by modifying the Least Significant Bits (LSB) of image pixels in accordance with the watermark bits. Spatial domain techniques are suitable for applications having

fragility a key requirement and as such are suited for authentication purposes. The spatial domain based data hiding schemes can be easily implemented and possess least design complexity. This method is suitable for fragility and some of the related schemes are reported in [23-25]. For robust watermark applications embedding is usually done in frequency coefficients which are obtained from the image by performing transforms like discrete cosine transform (DCT), Integer Wavelet Transform (IWT) and discrete wavelet transform (DWT). A robust watermarking scheme has been proposed in [25] and is based on difference of corresponding coefficients between two successive DCT blocks. The host image is first arranged into 8x8 blocks which is followed by application of DCT on each block. The embedding is carried out by modifying the difference between two corresponding coefficients of two neighbouring blocks. Similar other robust watermarking schemes are reported in [26-28]. For security purposes some of the watermarking schemes as reported in [29] also used an encryption technique. This security procedure ensures that if the unauthorized user somehow cracks the embedding algorithm, watermark extracted will not be in original form and will convey no information.

### 3. PROPOSED TECHNIQUE

In this section, the proposed watermarking technique is described in detail from embedding to extraction stage. The proposed scheme is a fragile watermarking technique for authentication and data integrity purposes based on spatial domain. This work proposes a block based watermarking algorithm involving mean based approach for embedding watermark. For the scheme, to ensure high level security the watermark is first encrypted using chaos map encryption algorithm.

#### 3.1 Embedding Algorithm

The generalized flow diagram of the proposed scheme is shown in Figure 1. The watermark embedding process starts with an encrypted watermark (which generally is a binary logo of size 64 x 64) and a gray scale cover image of size 512 x 512. The fragile watermark is embedded using the following steps:

**Step 1:** Apply chaotic encryption the watermark.

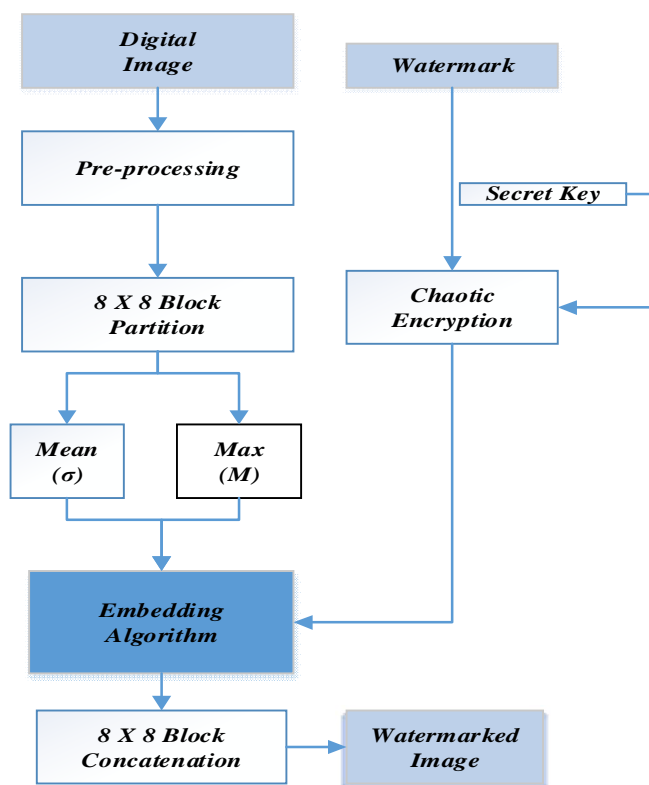


Figure 1. Block diagram for embedding watermark.

**Step 2:** Divide the cover image into 8 x 8 blocks and represent blocks by ' $\Pi_{xy}$ '.

**Step 3:** Calculate mean of the block. The mean is stored in variable, ' $\sigma$ '.

**Step 4:** Calculate maximum of the block. The maximum is stored in variable, ' $M$ '

**Step 4:** Apply embedding procedure to embed watermark as shown in Figure 2.

**Step 5:** Initialize two variables before start of embedding process:  $\alpha$  and  $\delta$ . These variables act as secret keys.

**Step 6:** The watermark bit is embedded by modifying the vales block by a calculated factor ' $\Delta$ ' calculated as:

$$\Delta = \sigma_n - \sigma \quad (1)$$

If  $w(a)$  is the a-th watermark bit, then embedding is done as follows:

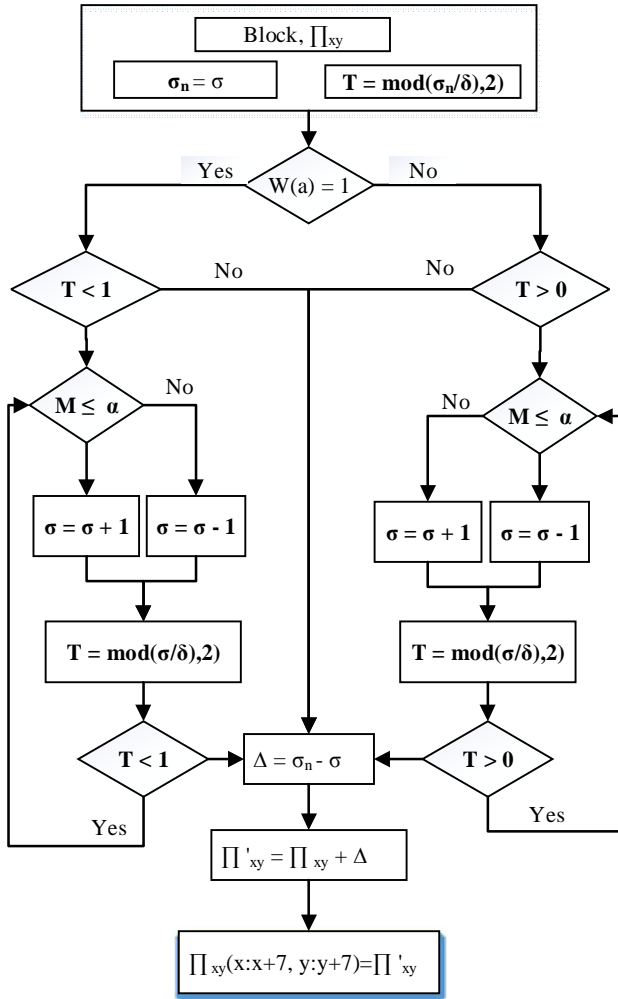


Figure 2. Flow of watermark embedding in a block.

**Step 7:** After embedding process is complete the modified block is obtained,  $\Pi'_{xy}$ .

**Step 8:** The resulting 8 x 8 blocks in step 7 replaces the corresponding coefficients in the 8 x 8 block. This is followed by joining 8x8 block to get final watermarked image.

### 3.2 Watermark Extraction

The watermark extraction process used in proposed fragile watermarking scheme is inverse of corresponding embedding process. Extraction of the fragile watermark logo is achieved after performing some necessary pre-processing operations on the watermarked image. After obtaining the 8 x 8 blocks as per the steps shown in Figure 1, watermark bit is extracted using the following equations:

$$\sigma = \text{mean}(\Pi'_{xy}) \quad (2)$$

$$W_e(a) = \text{mod}(\sigma/\delta, 2) \quad (3)$$

## 4. RESULTS AND DISCUSSION

In this section, results of the proposed watermarking scheme are presented by performing subjective and objective analysis. Several standard gray scale cover images of size N x N like plane, boat etc. are used for the analysis of the proposed scheme. Various test images of size 512 x 512 and watermark of size 64 x 64 chosen are shown in Fig. 3. To evaluate the perceptual quality of the watermarked image, the parameter like peak signal to noise ratio (PSNR) and similarity index (SSIM) are used [30]. Similarly, parameters like Bit error rate (BER) and Normalized Cross correlation (NCC) are used for analysing the fragility.

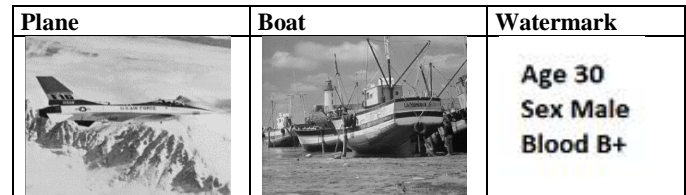


Figure 3. Medical images used in proposed scheme.

Fragility describes the resistance of the watermarking scheme against image manipulations due to attacks such as filtering, cropping, scaling, adding noise, and so on. The fragility is usually measured in terms of NCC and BER with respect to the original watermark and the extracted watermark in the presence of signal processing attacks. The value of BER should be as low as possible for a better watermarking scheme and if BER converges to zero then the original watermark is said to be completely recovered.

In this section the perceptual quality of the watermarked images has been analyzed and presented. The proposed scheme is analyzed for its performance using the medical general images as shown in Figure 4. The proposed watermarking scheme attains an average PSNR value around >50dB when a 64 x 64 watermark logo is embedded in an image.



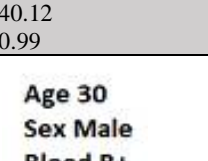
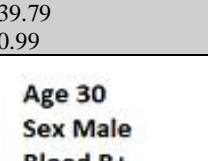
Watermarked Image		
		
PSNR (dB)	40.12	39.79
SSIM	0.99	0.99
Extracted Watermark	Age 30 Sex Male Blood B+	Age 30 Sex Male Blood B+
BER (%)	0	0
NCC	1	1

Figure 4. Watermarked images and extracted logos under no attack

For the cases like privacy and authentication the fragility of a watermarking scheme is the most important factor. The watermarked image is exposed to several attacks and the results hence recorded are analysed for fragility. Table 1, shows the objective results obtained after different attacks on the watermarked image.

**Table 1. Results of extracted watermarks in terms of NCC and BER values**

Attack Type	NCC	BER (%)
No Attack	1	0
Histogram Equalization	0.6955	52.667
JPEG (QF = 70 )	0.6574	56.778
Rotation (45o)	0.5947	60.071
Scaling down by 25%	0.6087	61.792
Smoothing Filter	0.7011	51.231
JPEG 2000 (CR = 8)	0.7162	50.891
Low Pass Filtering	0.6315	54.223
S & P Noise (v = 0.01)	0.6123	59.234
Gaussian Noise (v = 0.01)	0.5913	59.998
Sharpening	0.6671	54.483
Cropping (25%)	0.6022	59.843
Poisson Noise	0.5862	60.556
Gamma Correction	0.6722	54.332

From the results it is clear that the proposed algorithm offers high visual quality and fragility and thus can be used for authentication applications.

## 5. CONCLUSION

In this paper a fragile watermarking scheme has been proposed for securing digital information. In order to achieve the said goal a fragile watermark was embedded in the host image. The experimental results proved that the proposed shows high fragility against different attacks like resizing, cropping, scaling, filtering and other noise and compression attacks. The use of encryption ensures high level security of the private information and can hence be used for security purposes. The use of the proposed technique in authentication applications will ensure the privacy and integrity of the data.

## 6. ACKNOWLEDGEMENTS

This publication is an outcome of the R&D work undertaken project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation.

## REFERENCES

- [1] Roy, S. and Pal, A.K., "A blind DCT based color watermarking algorithm for embedding multiple watermarks," AEU-International Journal of Electronics and Communications, 72, 2017, pp.149-161.
- [2] Chen, J.X., Zhu, Z.L., Fu, C., Zhang, L.B. and Zhang, Y., "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," Communications in Nonlinear Science and Numerical Simulation, 23(1), 2015, 294-310.
- [3] S.A. Parah, J.A. Sheikh, A. M. Hafiz and G.M. Bhat, (2014a) 'Data hiding in scrambled images: a new double layer security data hiding technique', Computers and Electrical Engineering, Vol. 40, No. 1, pp.70-82, Elsevier.
- [4] J.A. Sheikh, S.A. Parah, A.M. Hafiz and G.M. Bhat, (2015a) 'A secure and robust information hiding technique for covert communication', International Journal of Electronics, Vol. 102, No. 8, pp.1253-1266, Taylor and Francis, UK.
- [5] F. Ahad, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2015b) 'On the realization of robust watermarking system for medical images', 12th IEEE India International Conference (INDICON) on Electronics, Energy, Environment, Communication, Computers, Control (E3-C3), 17-20 December, Jamia Millia Islamia, New Delhi, pp.1-6.
- [6] J. A. Akhoun, S.A. Parah, J.A. Sheikh, N. A. Loan and G.M. Bhat, (2015c) 'A High capacity data hiding scheme based on edge detection and even-odd plane separation', In India Conference (INDICON), 2015 Annual IEEE 2015 Dec 17 (pp. 1-5). IEEE.
- [7] F. Ahad, S.A. Parah, J.A. Sheikh, N. A. Loan and G.M. Bhat, (2015d) 'Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications. 2017 Apr 1;76(8):10599-633. Springer.
- [8] Shabir A. Parah, J.A. Sheikh and G.M. Bhat, (2015e) 'Hiding in encrypted images: a three tier security data hiding system', Multidimensional Systems and Signal Processing, September, Springer, DOI: 10.1007/s11045-015-0358-z.
- [9] Nasir Nabi Hurrah, Zubair Jan, Anil Bhardwaj, Shabir Ahmad Parah, Amit Kant Pandit, 2015. Oversampled Sigma Delta ADC Decimation Filter: Design Techniques, Challenges, Tradeoffs and Optimization. Proc. of RAECs UIET Panjab University Chandigarh.
- [10] S.A. Parah, J.A. Sheikh, J.A. Akhoun, N. A. Loan and G.M. Bhat, Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. Multimedia Tools and Applications. 2018 Jan 1;77(1):185-207., Springer, DOI: 10.1007/s11042-016-4253-x.
- [11] N. A. Loan, S.A. Parah, J.A. Sheikh, and G.M. Bhat, (2016b) 'Robust and blind watermarking technique in DCT domain using inter-block coefficient,' Digital Signal Processing, Elsevier, DOI: 10.1016/j.dsp.2016.02.005.
- [12] F. Ahad, S.A. Parah, J.A. Sheikh, N.A. Loan and G.M. Bhat, (2016c) 'A New Reversible and high capacity data hiding technique for e-healthcare applications', Multimedia Tools and Applications, Springer, DOI: 10.1007/s11042-016-4196-2.
- [13] Loan, N. A., Hurrah, N. N., Parah, S. A., & Sheikh, J. A. (2017). High capacity reversible stenographic technique based on image resizing and pixel permutation. In Image Information Processing (ICIIP), 2017 Fourth International Conference on (pp. 1-6). IEEE.
- [14] J.A. Sheikh, S.A. Parah and G.M. Bhat, (2016a) 'StegNmark: a joint stego-watermark approach for early tamper detection', Intelligent Techniques in Signal Processing for Multimedia Security, Vol. 660, Springer DOI: 10.1007/978-3-319-44790-2\_17.

- [15] Nasir N. Hurrah, Loan, N. A., Parah, S. A., & Sheikh, J. A. (2017). A Transform Domain Based Robust Color Image Watermarking Scheme for Single and Dual Attacks. In Image Information Processing (ICIIP), 2017 Fourth International Conference on (pp. 1-6). IEEE.
- [16] F. Ahad, N. A. Loan, S. A. Parah, J.A. Sheikh and G.M. Bhat, (2016a) 'Pixel repetition technique: a high capacity and reversible data hiding method for e-healthcare applications', Intelligent Techniques in Signal Processing for Multimedia Security, Vol. 660, Springer, DOI: 10.1007/978-3-319-44790-2\_17.
- [17] Parah, S. A., Sheikh, J. A., Akhoun, J. A., & Loan, N. A. (2018). Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication, Future Generation Computer Systems. <https://doi.org/10.1016/j.future.2018.02.023>.
- [18] F. Ahad, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2017) 'Hiding clinical information in medical images: a new high capacity and reversible data hiding technique', Journal of Biomedical Informatics, February, Vol. 66, pp.214-230 [online] DOI: <http://dx.doi.org/10.1016/j.jbi.2017.01.006> (accessed 21 September 2017).
- [19] Shabir A. Parah, J.A. Sheikh and G.M. Bhat, (2012b) 'On the realization of a secure, high capacity data embedding technique using joint top-down and down-top embedding approach', Elixir Comp. Sci. & Engg., Vol. 49, pp.10141-10146.
- [20] S. Parah, J. Sheikh and G.M. Bhat, (2012a) 'On the realization of secure and efficient data hiding system using ISB and LSB technique', Engineering E-Transaction, Malaysia, Vol. 7, No. 2, pp.48-53, ISSN: 1823-6379.
- [21] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2012c) 'Data hiding in ISB planes: a high capacity blind stenographic technique', in Proc. of IEEE Sponsored Intl. Conference INCOSSET-2012, Tiruchirapalli Tamilnadu, India, pp.192-197.
- [22] S. Parah, J. Sheikh and G.M. Bhat, (2013a) 'High capacity data embedding using joint intermediate significant bit and least significant technique', International Journal of Information Engineering and Applications, Vol. 2, No. 11, pp.1-11.
- [23] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2013b) 'Data hiding in color images: a high capacity data hiding technique for covert communication', Computer Engineering and Intelligent Systems, Vol. 4, No. 13, pp.113-118.
- [24] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2013c) 'On the realization of a spatial domain data hiding technique based on intermediate significant bit plane embedding (ISBPE) and post embedding pixel adjustment (PEPA)', Proceedings of IEEE International Conference on Multimedia Signal Processing and Communication Technologies-IMPACT 2013, (AMU, Aligarh 23-25 November) pp.51-55.
- [25] S.A. Parah, J.A. Sheikh and G.M. Bhat, (2014b) 'A secure and efficient spatial domain data hiding technique based on pixel adjustment', American Journal of Engineering and Technology Research, US Library Congress, (USA), Vol. 14, No. 2, pp.38-44.
- [26] Hurrah, N. N., Loan, N. A., Parah, S. A., Lee, J. W., Sheikh, J. A., & Bhat, G. M. (2018). Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption. IEEE Access, 6, 19876-19897.
- [27] N. A. Loan, S.A. Parah, J.A. Sheikh and G.M. Bhat, (2017) 'Utilizing neighbourhood coefficient correlation: a new image watermarking technique robust to singular and hybrid attacks', Multidimensional Systems and Signal Processing, DOI: 10.1007/s11045-017-0490-z.
- [28] J.A. Sheikh, S.A. Parah, U.I. Assad and G.M. Bhat, (2016b) 'Realization and robustness evaluation of a blind spatial domain watermarking technique', International Journal of Electronics, DOI: 10.1080/00207217.2016.1242162.
- [29] Shah, A. A., & Parah, S. A. (2017). Chaos based novel cryptographic technique based on a new logistic map. International Journal of Social Computing and Cyber-Physical Systems, 2(1), 73-94.
- [30] Zhou, W., A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. "Image Quality Assessment: From Error Visibility to Structural Similarity." IEEE Transactions on Image Processing. Vol. 13, Issue 4, April 2004, pp. 600-612.