A Dual Watermarking Scheme for Ownership Verification and Pixel Level Authentication

Shivendra Shivani
National Institute
of Technology
Allahabad, India
shivendrashivani@gmail.com

Priyanka Singh
Indian Institute
of Technology
Roorkee, India
priyankaap@gmail.com

Suneeta Agarwal
National Institute
of Technology
Allahabad, India
suneeta@mnnit.ac.in

ABSTRACT
Breaches of multimedia security are increasing day by day as advancement in technologies have tightly coupled the globe and promoted easy sharing of multimedia content in no loss of time. A dual watermarking scheme ascertaining the rightful ownership and integrity of images is proposed here. A gray scale logo used as copyright information of the owner is embedded imperceptibly into the singular values of the cover image in multiple locations. The multiplicity of embedding ensures extraction of embedded information even in worst tampered scenarios and hence, prove the rightful ownership. The proposed scheme also performed pixel wise authentication which fetched the advantage of accurate tamper localization in case of alterations. The visual quality of the watermarked image is maintained high as indicated by the high Peak-Signal-to-Noise-Ratio(PSNR) values. The robustness of the scheme is tested against comprehensive set of attacks and evaluated by various objective evaluation parameters. Objective evaluation parameters close to their ideal values demonstrate the efficacy of the proposed scheme over other existing state of art approaches.

CCS Concept
Security and privacy→ Digital rights management

Keywords
Dual Watermarking; Rightful Ownership; Integrity; Authentication; Tamper Localization; Peak-Signal-to-Noise-Ratio(PSNR); Objective evaluation parameters.

1. INTRODUCTION
The advancement in technologies has proved as boons to society as they allow easy sharing, storage and redistribution of multimedia content with much less efforts and time constraints. But as advantages increase, so are the threats too. Misuse of multimedia content, illegal copying without obtaining any legal rights, limitless redistribution etc. raise the issue of copyright protection. Schemes assuring such protection like steganography, cryptography, watermarking etc. are being inculcated towards this end. Cryptography faces the disadvantage that data once decrypted is no far protected and can be misused again. Steganography involves secret hiding where the very existence of communication is hidden.

ICCAE '17, February 18-21, 2017, Sydney, Australia

DOI: http://dx.doi.org/10.1145/3057039.3057042

1.1 Classification of Watermarking Schemes
Up to now, two traditionally-used strategies, spatial domain [1] and transform domain [2][3] techniques have been developed for digital image watermarking. The former category is designed to insert directly a watermark into the pixels of the cover image by a factor such that it would lead to fair-quality watermarked image. The second approach is designed to embed a watermark into the frequency-domain of the cover images by for taking advantage of perceptual properties of transformations. These types of watermarking schemes have good performance of robustness in comparison to the most common signal processing manipulations such as JPEG compression, filtering, and addition of noise, hence it can be used for ownership assertion. For proving rightful ownership, watermarking is considered to be one of them embedded into the cover multimedia content maintaining the visual quality of the cover content. On the receiver end, the embedded information can be extracted to prove the rightful ownership, [4]-[6]. The secret information may be either random sequence numbers, copyright logos of the firms or any other information related to the transaction like transaction dates, ownership identifiers, information about the creators of the work etc. [7]. Watermarking has varied applications like ownership assertion, authenticity of content, transaction tracking, proof of ownership etc. Based on the application and resistance of watermark, watermarking schemes can be broadly classified as fragile schemes, semi-fragile schemes and robust schemes. Fragile schemes are those schemes that remain vulnerable to slightest tampers and aim to detect altered regions in case of tampering. Robust watermarking schemes are those that have the ability to survive most of malicious and incidental manipulations and still be able to extract the copyright logo to prove the rightful ownership. Semi fragile schemes are intermediary schemes between the two extremes. They remain robust to a certain threshold limit and thereafter become vulnerable. Varied combinations of watermarking schemes targeting multiple functionalities are termed as dual watermarking schemes. Robust and fragile watermarks are embedded into the same cover image to achieve multiple objectives. They may be embedded into separate regions of the cover image or may be dependent or independent of the order of embedding. Though a variety of robust watermarking schemes [4]-[6],[8]-[12] in spatial as well as frequency domain have already been proposed in the literature that aim at proving rightful ownership. But still they could not

handle malicious attacks. Fragile schemes have the capability of detecting even slight tampers too. Fragile watermarks remain vulnerable to attacks and change on manipulations [7]. However, the incidental manipulations could not be handled by such schemes. Hence, a solution evolved as semi fragile watermarking schemes that could handle incidental manipulations and overcome malicious one too up to a certain threshold. Dual watermarking schemes are emerging as multi objective solutions to it. An authentication based scheme assuring integrity check has been proposed in[13]. It could detect tampered regions but accuracy of localization was quite low. In [10],[11], the localization accuracy was improved upon but recovery information was not incorporated. Hence, dual watermarking schemes is serving as an active research area. Feature-based watermarking has raised a number of available algorithms over the last few years. For solving watermark synchronization problems, feature region detection is the preferred strategy to resist against local geometric distortions. Generally speaking, content-based synchronization watermarking schemes follow the same basic process: detected feature points are localized at the local maxima while non maxima suppression that eliminates pixels that are not local maxima, and the final set of features is determined by analysis of threshold. Afterwards, extracted feature points are applied to identify regions for watermark insertion in the host image. At the receiver side, the feature points are detectable without synchronization error. The observation of feature-based synchronization has resulted in various algorithms known as region based watermarking. The feature points-based approach is a technique using localized watermarking algorithms. It discovers the watermark using stable feature points of images, where the watermark is independently inserted into the corresponding each local region. Hence the feature-based process can be invariant to local geometrical deformations so that it is an encouraging approach to solve the robustness against geometrical deformations in the watermarking scheme with blind detection. Robust watermark and fragile watermark both are sufficient enough to provide ownership assertion and integrity verification separately, respectively. There are very few effective state of art blind watermarking algorithms present in literature which have functionalities of both watermarking schemes. In this paper an effective blind watermarking scheme has been proposed which can provide the protection for the ownership of cover image with pixel wise authentication. The rest of the paper is organized as follows: section 2describes the proposed approach in detail, experimental results are presented in section 3. Conclusions along with the scope of future work has been included in section 4 followed by references.

1.2 The Proposed Scheme

The proposed watermarking scheme provides dual functionalities of ownership assertion and authentication. It thus consists of following main phases: embedding of copyright information, generation and embedding of authentication information, ownership verification through extraction of copyright information and tamper detection. The details of the phases are as follows:

1.3 Embedding of Copyright Information

The embedding of copyright information is done in the frequency domain. This facilitates the imperceptibility of the watermarked image as well as enhances the robustness of the proposed scheme against various incidental as well as malicious manipulations. Consider a gray scale cover image (I) having M rows and N columns. Let the intensity value of each pixel be denoted by Pn_[0 − 255] where n = 1; 2; 3; : : :M × N. A binary copyright logo (W)of size M×N/4 as watermark image is embedded in frequency domain of the cover image so as to handle worst tamper scenarios. The detailed flowchart of copyright information embedding and authentication bit generation/embedding is shown in Fig. 1. Detailed algorithm for copyright information embedding is shown in Algorithm 1.

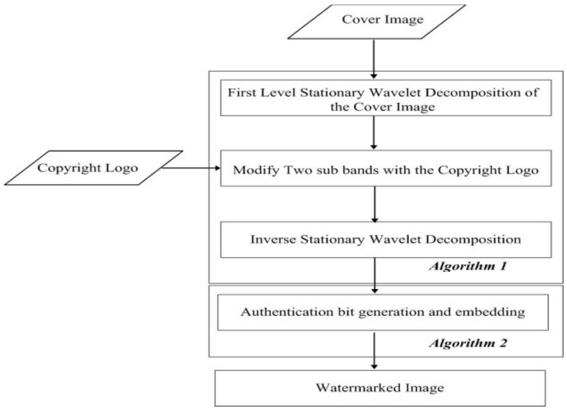

Figure 1.Embedding of copyright information and authentication bit

Algorithm 1 Embedding of copyright information

INPUT: I *and* W.

OUTPUT: I_c.

(1) T is a temporary variable.

(2) $|x|$ returns the absolute value of x

$[A^1\ A^2\ A^3\ A^4] \leftarrow DWT(I)$
for $i \leftarrow 1$ to $\frac{M \times N}{4}$ **do**
  for $j \leftarrow 1$ to $\frac{M \times N}{4}$ **do**
    if $W(i,j) = 1$ **then**
      if $A^3(i,j) \leq A^2(i,j)$ **then**
        $T \leftarrow |A^2(i,j)| - |A^3(i,j)|$
        $A^3_w(i,j) \leftarrow T + A^3(i,j)$
        $A^3_w(i,j) \leftarrow A^3_w(i,j) + \frac{A^2(i,j)+A^3(i,j)}{2}$
      end if
    else
      if $A^2(i,j) \leq A^3(i,j)$ **then**
        $T \leftarrow |A^3(i,j)| - |A^2(i,j)|$
        $A^2_w(i,j) \leftarrow T + A^2(i,j)$
        $A^2_w(i,j) \leftarrow A^2_w(i,j) + \frac{A^2(i,j)+A^3(i,j)}{2}$
      end if
    end if
  end for
end for
$I_c \leftarrow IDWT([A^1\ A^2_w\ A^3_w\ A^4])$
return I_c

1.4 Generation and Embedding of Authentication Information

Once we get the I_c, it will be treated like input image for next Algorithm 2. In this algorithm a self-embedding fragile watermark is generated for each pixel and embedded in first LSB of that pixel only. By this way we can achieve good imperceptibility with high tamper detection capability. Since watermark embedding and extraction algorithm are well known hence to provide security

here two secret keys K1 and K2 are used to generate these authentication bits.

Algorithm 2 Generation and embedding of authentication information

INPUT: I_c.
OUTPUT: I_w.
(1) β and γ are two empty vector of size 1×5 where β_m indicates the m^{th} bit of β.
(2) $b(P, m)$ indicates the M^{th} bit of P^{th} pixel.

$I_w \leftarrow I_c$
Generate a random vector R_1 of length $1 \times M$ using secret key (K_1)
$R_1 \leftarrow (R_1 \times 1000) mod(M)$
Generate a random vector R_2 of length $1 \times N$ using secret key (K_2)
$R_2 \leftarrow (R_2 \times 1000) mod(N)$
for $i \leftarrow 1$ to M **do**
  for $j \leftarrow 1$ to N **do**
    $R_q \leftarrow I_c(i, j)$
    $\beta \leftarrow$ Obtain five most significant bits $b(R_q, 8)$, $b(R_q, 7)$, $b(R_q, 6)$,$b(R_q, 5)$,$b(R_q, 4)$ of the Input image pixel $(I_c$
    $P_q = I_c(R_1(i), R_2(j))$
    $\gamma \leftarrow$ Obtain five most significant bits $b(P_q, 8)$, $b(P_q, 7)$, $b(P_q, 6)$,$b(P_q, 5)$,$b(P_q, 4)$ of the Input image pixel $(I_c$
    $A_u = \sum_{m=1}^{5} XOR(\beta_m, \gamma_m) mod 2$
    $b(I_w(i, j), 1) \leftarrow A_u$
  end for
end for
return I_w

1.5 Ownership Verification

To identify the rightful owner, the copyright information is extracted from the suspected watermarked image (I_w). If the extracted watermark logo matches with the original one then the ownership is confirmed else there is a dispute. The detailed procedure of copyright information extraction and tamper detection are shown in Fig. 2. Algorithm 3 demonstrates the extraction of copyright information in detail. This extracted watermark is then compared with the original watermark to prove the rightful ownership.

1.6 Tamper Detection

To detect the tampered regions, first of all the authentication bit is calculated for each pixel of the watermarked image.

Algorithm 3 Ownership Verification

INPUT: I_w.
OUTPUT: W_e.
(1) W_e is empty matrix of size $\frac{M \times N}{4}$.

$[A^1\ A^2\ A^3\ A^4] \leftarrow DWT(I_w)$
for $i \leftarrow 1$ to $\frac{M \times N}{4}$ **do**
  for $j \leftarrow 1$ to $\frac{M \times N}{4}$ **do**
    if $A^3(i, j) \geq A^2(i, j)$ **then**
      $W_e(i, j) \leftarrow 1$
    else
      $W_e(i, j) \leftarrow 0$
    end if
  end for
end for
return W_e

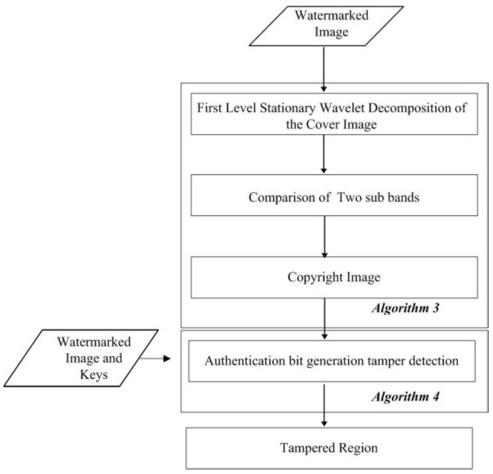

Figure 2. Extraction of copyright information and tamper detection

Then the embedded authentication bit is extracted from each of watermarked image pixel. The calculated authentication bit and the extracted authentication bit both are matched. If a mismatch arises, then it indicates the tampered pixels and reflected by white regions in tamper detected image. For matched pixels, it is represented by black region. The step wise procedure is shown in Algorithm 4.

2. EXPERIMENTAL RESULTS AND COMPARISON

The proposed scheme presented in this paper has been implemented using MATLAB R2013a. To test the efficacy of the proposed scheme, experiments have been performed on a large dataset of gray scale cover images and binary watermarks. Some are shown in Fig. 3 and Fig. 4.

Algorithm 4 Tamper Detection

INPUT: I_w, K_1 and K_2.
OUTPUT: T_r.
(1) T_r is matrix of size $M \times N$ with all values as zeros .

for $i \leftarrow 1$ to $M \times N$ **do**
  for $j \leftarrow 1$ to $M \times N$ **do**
    Recalculate the A_u for $I_w(i, j)$ using Algorithm 2 and K_1 & K_2.
    $B \leftarrow b(I_w(i, j), 1)$
    if $B \neq A_u$ **then**
      $T_r(i, j) \leftarrow 1$
    end if
  end for
end for
return T_r

Figure 3. Cover image

The imperceptibility of the watermarked image with respect to the original cover image has been measured using Peak-Signal-to-Noise-Ratio(PSNR) metric. The proposed scheme attains good in distinguishability of the watermarked image from the cover image as indicated by the values tabulated in Table I. Since proposed

approach uses binary images as watermark hence various objective evaluation parameters are used to measure the similarity between extracted and original watermark images.

Figure. 4. Copyright Logos (Copyright 1, Copyright 2 and Copyright 3)

Table 1.PSNR metric values for watermarked images

Cover Image	Lena	Baboon	Barbara	Ship
PSNR Value	55.65	56.78	54.34	54.67

Table 2.Various objective evaluation measures between recovered and original copyright logo for histogram equalization, gaussian(VAR=0.01) and JPEG(QF=50)

Objective Evaluation Measures	Average values of copyright logo		
	Histogram equalization	Gaussian	JPEG
Precision	.9562	0.7671	0.6009
Recall	0.9232	0.8322	0.7218
NRM	0.1157	0.3205	0.4151
SSIM	.801	0.7849	0.7381
Specificity	0.8501	0.7558	0.4855
BCR	0.8957	0.7524	0.6609

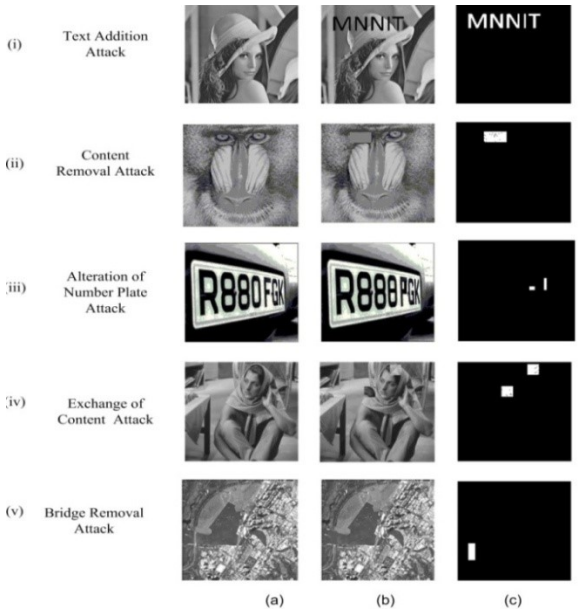

Figure 5. (a)Original Image, (b)Attacked Watermarked Image, (c)Tamper Detected Image

Analysis for quality of extracted watermark with respect to the original one have been shown in Table 2 for three types of modifications namely histogram equalization,Gaussian noise insertion and JPEG compression on watermarked images respectively. Table 2 show the robustness of the proposed scheme against various types of intentional or unintentional attacks as most of the parameters reach towards their ideal value.To assess the tamper detection feature of the proposed scheme, a number of alterations have been done on the various cover images. Some are depicted in Fig. 5. The tamper hasbeen detected on pixel basis. The white regions depict the altered regions whereas the black regions show the unaltered regions. The tamper detection results are tabulated in Table 3.

2.1 Comparison

Proposed approach is a fusion of the functionalities of fragile watermarking scheme and robust watermarking scheme hence it is compared with the various state of art approaches of same functionalities separately. To illustrate the efficacy for tamper detection of the proposed scheme over other state of art algorithms[12]-[17]various object removal and additional attack is performed and quantitative results are shown in Table 4.

Table 3Tamper detection results

Cover Image	Detected Pixels	Total Pixels Altered	Detection Rate
Lena	1967	2019	97.42
Baboon	797	816	97.67
NumPlate	109	111	98.19
Barbara	820	834	98.32
Sat.Image	519	530	97.92

Since proposed approach is suitable for gray scale cover images hence the comparison of imperceptibility between various sets of original cover images and their corresponding watermarked images has been done using PSNR metric with values tabulated in Table 5.

Table 4 Comparative performance based on tamper detection rate(%)

Attack	Our	[12]	[13]	[14]	[15]	[16]	[17]
Object addition	95.77	90.34	93.12	85.74	95.23	90.64	88.45
Object Removal	97.42	91.51	94.90	85.01	96.94	91.39	89.17

Table 5 Comparative performance based on PSNR between cover image And watermarked image.

Image	Our	[1]	[5]	[8]	[9]
Lena	56.3	46.3	39.12	45.74	35.23
Baboon	55.2	45.7	44.90	45.01	36.94
NumPlate	55.87	47.8	44.38	40.71	35.17
Barbara	54.12	40.83	46.38	40.71	35.17
SatImage	53.79	46.83	44.38	40.71	38.14

3. CONCLUSION

A dual watermarking scheme integrating the concepts of ownership verification along with tamper detection has been proposed here. The imperceptibility of the watermarked images as well as the extracted binary logos was found to be satisfactorily well as evaluated by the PSNR and various objective evaluation parameters. The robustness of the scheme has also been validated against comprehensive set of attacks. Hiding in multiple locations of the cover image enhanced the robustness property of the

scheme. The authentication was performed at pixel level and the tamper detection accuracy tested against various attacks was computed on pixel basis. The future study will focus on incorporating the recovery ability for the tampered regions in the proposed scheme so that it could serve for restoration purposes too.

4. REFERENCES

[1] Takahashi A., Nishimura R., and Suzuki Y. 2005. Multiple watermarks for stereo audio signals using phase-modulation techniques. IEEE Transactions on Signal Processing, 53:806-815.

[2] Kim T. Y., Choi H., Lee K., and T. Kim 2004. An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark. IEEE SignalProcessingTellers,2:375-377.

[3] Cruz-Ramos, C., Reyes-Reyes, R., Nakano- Miyatake, M., &Prez-Meana, H. (2010). A Blind Video Watermarking Scheme Robust To Frame Attacks Combined With MPEG2 Compression. Journal of applied research and technology, 8(3),323-337.

[4] B. Hennelly and J. T. Sheridan. Optical image encryption by random shifting in fractional fourier domains. Opt. Lett., 28(4):269–271, Feb 2003.

[5] Ran Tao, Yi Xin, and Yue Wang. Double image encryption based on random phase encoding in the fractional fourier domain. Opt. Express, 15(24):16067–16079, Nov 2007. Spector, A. Z. 1989.

[6] Priyanka Singh and Suneeta Agarwal. An efficient fragile watermarking scheme with multilevel tamper detection and recovery based on dynamic domain selection Tools and Applications, pages 1–30, 2015.

[7] Priyanka Singh and Suneeta Agarwal. A region specific robust watermarking scheme based on singular value decomposition. In Proceedings of the Fifth International Conference on Security of Information and Networks,SIN '12, pages 117–123, New York, NY, USA, 2012. ACM.

[8] Hone-Ene Hwang and Pin Han. Fast algorithm of phase masks for image encryption in the fresnel domain. J. Opt. Soc. Am. A, 23(8):1870–1874,

[9] Priyanka Singh and Suneeta Agarwal. A region specific robust watermarking scheme based on singular value decomposition. In Proceedings of the Fifth International Conference on Security of Information and Networks,SIN '12, pages 117–123, New York, NY, USA, 2012. ACM.

[10] Shivendra Shivani, Anoop Patel, Sushila Kamble and Suneeta Agarwal. An effective fragile watermarking scheme based on ARA bits. Proceedings of the 2011 International Conference on Communication, Computing & Security, ICCCS, Odisha, India, February 12-14, 221–226, 2011.

[11] Shan Suthaharan. Fragile image watermarking using a gradient image for improved localization and security. Pattern Recogn. Lett., 25(16):1893–1903, December 2004.

[12] G. Unnikrishnan, J. Joseph, and K. Singh. Optical encryption by double random phase encoding in the fractional fourier domain. Opt. Lett.,25(12):887–889, Jun 2000.

[13] P.W. Wong and N. Memon. Secret and public key image watermarking schemes for image authentication and ownership verification. Image Processing, IEEE Transactions on,10(10):1593–1601,Oct2001.

[14] Durgesh Singh, Shivendra Shivani, Suneta Agarwal. Quantization based Fragile Watermarking using Block wise Authentication and Pixel wise Recovery scheme for Tampered Image. In International Journal of Image and graphics, world scientific Vol. 13(2), 2013.

[15] Cox I. J., Miller M. L., and Bloom J. A. 2001. Digital Watermarking. San Francisco, CA: Morgan Kaufman.

[16] Shivendra Shivani, Suneeta Agarwal Novel Basis Matrix Creation and Preprocessing Algorithms for Friendly Progressive Visual Secret Sharing with Space-Efficient Shares, MULTIMEDIA TOOLS AND APPLICATIONS Springer, Vol 75, No. 7.

[17] Deng C., Gao X., Li X. and Tao D., 2009. A local Tchebichef moments based robust image watermarking. SignalProcess.,89(8):15311539.