AN APPROXIMATION APPROACH FOR DIGITAL IMAGE OWNER IDENTIFICATION USING HISTOGRAM INTERSECTION TECHNIQUE

MIR SHAHRIR EMAMI1, GHAZALI BIN SULONG1 AND SALBIAH BINTI SELIMAN2

1Department of Computer Graphics and Multimedia
Faculty of Computer Science and Information Systems
2Department of Management
Faculty of Management and Human Resource Development
Universiti Teknologi Malaysia
81310, Skudai, Johor, Malaysia
shemami85@yahoo.com

Received April 2011; revised August 2011

ABSTRACT. Researchers have documented a wide variety of attacks against digital image watermarking techniques. Meanwhile, many strong attacks have been appearing at a reasonable rate. The investigations emphasize that modelling of the behaviours regarding such attacks is difficult. Studies have revealed that existing watermarking algorithms have a tendency to be severely affected by such strong attacks which results in destroyed watermarks. Hence, in the influence of such attacks, the ownership identification of the property cannot be established. This paper proposes an approximation approach for identification of the rightful owner of the property utilizing the remaining information of the attacked watermarks regardless of the attack behaviour. Here, we coupled the BiSB (Duo-ISB-Bit-Plane) watermarking algorithm together with the HI (Histogram Intersection) technique in order to identify the ownership of the property. In BiSB approach, while the main watermark delivers the ownership identification information, the sub-watermark which is a bit-pattern histogram, is the statistical information regarding the main watermark. In addition, three bit-pattern histograms namely, original, extracted and computed sub-watermarks have been used for approximation purpose. An investigation has been achieved using a standard Lena gray-scale host image of 512 × 512 pixels, a trademark image of 38 × 89 pixels as a sub-watermark and JPEG2000 lossy compression, Cropping and Reset Removal watermarking attacks. The results have revealed that the proposed approach highly balanced the trade-off between imperceptibility and robustness. This was successfully achieved by preserving the quality of the watermarked image and, at the same time, identifying the ownership of the property even though the attack totally corrupted the embedded watermarks.

Keywords: Watermarking, Ownership identification, Histogram intersection, Approximation approach, LSB, ISB, EISB, BiSB

1. Introduction. Nowadays, various sources such as scientific experiments, satellites, digital cameras and biomedical imaging are generating digital images at an explosive rate. Meanwhile, the rate of ever-increasing Web users has become uncontrollable and multimedia technologies advance at a very fast rate. Such a situation results in uncontrollable digital distributions of digital image assets through the Internet and other networks. In actual fact, these digital image properties should be used by authorized users only.

A review of the literature shows that digital watermarking techniques in terms of the domain can be categorized into two: the transform-domain and the spatial-domain [1,4,6,10,12,13,29,41]. Both techniques have been widely used by researchers. Meanwhile,
according to Bender et al. [14], watermarking techniques encounter restrictions. For example, each spatial-domain approach has its own weaknesses. In the least significant bit-planes approach, there were no highly embedding errors during the embedding stage. Hence, many researchers employed least significant bit-planes for data hiding [3,11,31-33]. Unfortunately, the least significant bit-planes do not contain significant visual information. So, at the same time, the embedded watermark may be easily corrupted or replaced by unauthorized users without perceptible visual effects. Therefore, other researchers used ISB bit-planes in both spatial and transform domains [8,10,30,34,35] to improve this drawback. Nevertheless, the watermarked image suffers from poor quality when the watermarking algorithm selects higher bit-planes in ISB approaches. According to Rabah [36], watermarked image would look similar to its original host image if the used bit-plane for information hiding is lower than the 5th. However, choosing higher bit-planes could result in higher robustness. In other words, when the watermarking algorithms select higher bit-planes for watermark embedding, the image quality decreases as the robustness increases. Meanwhile, any attack on watermarked image can produce more degradation effects for its quality and make the attacked watermarked image useless and unproductive for piracy. This can be interpreted as a higher robustness. On the other hand, selecting lower bit-planes brings about less degradation effects and less robustness because the embedded watermark can be simply corrupted or replaced by malicious users without any visual effects. To come up with this problem, EISB technique [8,10,29] decreases the degradation effects of the watermarked image by preserving the watermarked pixels very close to the respective original values. Although EISB improved ISB technique in terms of visual degradation effects, there were still weaknesses. As said somewhere else [6], if higher bit-plane is used, a higher quality watermarked image is produced but robustness becomes low. However, if a lower bit-plane is used, the robustness becomes high but the quality of the watermarked image becomes low. Thus, the favorable results cannot be obtained in both robustness and imperceptibility in the EISB. To address this weakness, BiISB (Duo-ISB-Bit-Plane) approach [6] was proposed. In this method, both higher and lower bit-planes have been used to utilize the same EISB technique. In addition, in order to keep a higher quality of the watermarked image, only one bit of the watermark bit stream is embedded within each host image pixel. The bits pertaining to the sub-watermark must be embedded between the bits that belong to the main watermark.

1.1. BiISB watermarking approach revisited. Histogram, which has been described in the literature as a graphical representation of tabulated frequencies in bars display, has been widely applied by researchers in data analysis, for example in [16-19], in order to demonstrate the major features of the distribution of the data. The BiISB approach [6] utilizes this application of histogram. The BiISB approach can be depicted in Figure 1. This figure demonstrates that in BiISB scheme the main watermark and its sub-watermark are embedded in the host image pixels concurrently. The main watermark is usually much larger than its sub-watermark. In this approach, with the purpose of embedding the sub-watermark, a period which we called Distance is used as a secret key. The Distance refers to the distance between any of the two bits of the sub-watermark in the host image pixels. For example, if the Distance is 100, and the first embedding position of the embedded sub-watermark bit is 200, then other bits of the sub-watermark bit stream must be embedded in the host image with pixel positions (PixPositions) of 300, 400, 500, etc. This means the sub-watermark embedding positions must satisfy Equation (1).

\[
\text{mod} (\text{PixPosition}, \text{Distance}) = 0
\]
Figure 1. BiISB embedding scheme. BiISB approach utilizes the multiple watermarks technique such that two related watermarks are embedded in the host image. The main watermark is embedded within a low-order ISB bit-plane (WP) and its sub-watermark is embedded within a high-order ISB bit-plane (HP).

Table 1 shows the binary bit-patterns and their representation values in BiISB approach. For each bit-pattern in Table 1 we considered 2 bytes so for bit-pattern length 2, i.e., $\beta = 2$ the total memory usage was $2^2 \times 2 = 8$ bytes, i.e., eight bytes, and for $\beta = 3$ the total memory usage was $2^3 \times 2 = 16$ bytes, i.e., sixteen bytes and so on. By counting these bit-patterns in the main watermark bit stream content, a bit pattern histogram can be drawn for this watermark. Figure 2 shows the proposed bit-pattern histograms of four different watermarks using four bit-pattern lengths ($\beta = 2$, $\beta = 3$, $\beta = 4$ and $\beta = 5$).

<table>
<thead>
<tr>
<th>bit-Pattern Length ($\beta$)</th>
<th>Binary bit-Patterns</th>
<th>Decimal Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>00,01,10,11</td>
<td>0,1,2,3</td>
</tr>
<tr>
<td>3</td>
<td>000,001,010,011,100,101,110,111</td>
<td>0,1,2,3,4,5,6,7</td>
</tr>
<tr>
<td>4</td>
<td>0000,0001,0010,0011,0100,0101,0110,0111,1000,1001,1010,1011,1100,1101,1110,1111</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15</td>
</tr>
<tr>
<td>5</td>
<td>00000,00001,00010,00011,00100,00101,00110,00111,01000,01001,01010,01011,01100,01101,01110,01111,10000,10001,10010,10011,10100,10101,10110,10111,11000,11001,11010,11011,11100,11101,11110,11111</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31</td>
</tr>
</tbody>
</table>
1.2. Attacks on watermarking schemes. Watermark attacks are either intentional or unintentional removal, modification or replacement of the embedded watermark. An unauthorized duplication of a watermarked image can also be considered as a watermark attack. The quality of the watermarked image is usually degraded if it is attacked. However, the major goal of the watermarking attacks is to remove the embedded watermark without degrading the watermarked image quality [9].

2. Problem Statement. Researchers have reported numerous diversities of attacks against watermarking approaches [6,9,27,39,40]. This reveals that some attacks have complex behaviours so they are too complex to model. Meanwhile, according to Licks and Jordan [15], not enough effort has been put to produce a theory for modelling of geometric attacks. In actual fact, proposing a standard model for geometric attacks has become an open problem [37] and subsequently information hiding approaches which can robustly withstand against all geometrical attacks have become open problems as well [38]. Moreover, the ever-growing upcoming watermarking attacks are uncontrollable and modelling of such attacks is not possible as their behaviour is unknown. Furthermore, when the attacking strategy is smart enough (such that it can totally corrupt the embedded watermarks with low-degradation effects on the watermarked image), the embedded watermarks could not be extracted or recovered properly, so the ownership identification of the property cannot be established. Besides, high imperceptibility is needed in a watermarking technique for many real-time applications such as clinical applications [42,44] and photography. Otherwise, the watermarking technique cannot be used for such applications. For example, in the Blocked-based Biased-EISB watermarking approach [43], the imperceptibility of the approach is marginally acceptable; however, it is not adequate for many real-time applications. All these issues compel us to think of other approaches which can help us to identify the ownership of the digital image asset even though it has been affected by any attack regardless of the attack’s behaviour and, at the same time, highly preserve the quality of the host image. Now the question is: How can we balance the trade-off between imperceptibility and robustness by preserving the quality of the watermarked image and, at the same time, identifying the ownership of the property using the remaining information when the embedded watermark has been totally corrupted in the influence of severe watermarking attacks?

3. Proposed Scheme. In this section, an approximation approach is proposed based on the Histogram Intersection (HI) technique introduced by Swain and Ballard [22]. Here, three bit-pattern histograms are used to approximate the ownership identification of the
attacked watermarked image. These histograms are original sub-watermark, extracted sub-watermark and computed sub-watermark and for simplicity they are represented by $H_u$, $H_v$ and $H_w$ respectively. We utilized the HI technique in order to find the degree of similarity between these histograms. The following figure illustrates the relationship between these histograms.

![Histogram relationship triangle (HRT)](image)

**Figure 3.** Histogram relationship triangle (HRT)

Let $HI_w$, $HI_u$, $HI_v$ be the similarity rates of $H_u$ and $H_v$, $H_u$ and $H_w$, and $H_v$ and $H_w$ respectively. In order to find the degree of similarity between each pair of the mentioned histograms, the HI technique [22] given in Equation (2) is used,

$$HI = \sum_{i=0}^{\xi-1} \min(h_M(i), h_T(i))$$

(2)

where $HI$ indicates the histogram intersection, $h_M$ and $h_T$ denote normalized histograms of target image and model image respectively, and $\xi$ indicates the number of components in each of $h_M$ and $h_T$. When $HI = 1$ the target image and the model image are identical because the matching rate between their corresponding histograms are maximum and when $HI = 0$ the target image and the model image are totally distinct because the matching rate between their corresponding histograms are minimum.

The novelty of the proposed scheme is in twofold as follows. Firstly, the owner identification process of the attacked watermarked image was based on the statistical information of the two related embedded watermarks so it was independent from the watermarking attack behaviour. This means, there is no need to model the behaviour of the watermarking attack. This can be more useful when it is too complex to model some severe attacks or when the attack behaviour is unknown. Secondly, the proposed scheme was successful to preserve the quality of the property during the watermarking process. In conclusion, the proposed approximation approach (Approximated BiISB) can highly balance the trade-off between imperceptibility and robustness requirements.

3.1. **Conjecture.** The following events are some of the possible scenarios that might occur:

- If $HI_w = HI_u = HI_v = 1$, this means all three original, extracted and computed sub-watermarks are identical. This can be interpreted that the watermarked image 100% belongs to the rightful owner. However, this scenario is almost impossible to achieve after the attacking procedure.
- If $HI_w = HI_u = HI_v = 0$, this means all three sub-watermarks are distinct. This reflects that the owner of the watermarked image cannot be identified.
- If $HI_w = HI_u = HI_v = 0.5$, this indicates there is 50% chance that the property belongs to the rightful owner.
- If $HI_w > 0.5$, $HI_u = HI_v = 0$, this means there are more than 50% chances that the extracted sub-watermark is intact. However, the extracted main watermark has been totally destroyed.
Figure 4. Proposed extracting scheme

- If $HI_{uw} > 0.5$, $HI_{uw} = HI_{uw} = 0$, can be interpreted there are more than 50% chances that the extracted main watermark is intact. However, the extracted sub-watermark has been totally destroyed.
- If $HI_{uw} = 1$, $HI_{uw} = HI_{uw} = 0$, this indicates that the extracted main watermark and sub-watermark are closely related. However, both of them are totally distinct from the original histogram so the property belongs to other owner.

Now let $P_{HI}$ be the approximate value which shows the ownership probability or ownership degree of the digital watermarked property as represented in Equation (3),

$$P_{HI} = \begin{cases} 
0 & \text{if } HI_{uw} = 1 \land HI_{uw} = HI_{uw} = 0 \\
HI_{uw} & \text{if } HI_{uw} > 0 \land HI_{uw} > HI_{uw} \land HI_{uw} > HI_{uw} \\
HI_{uw} & \text{if } HI_{uw} > 0 \land HI_{uw} > HI_{uw} \land HI_{uw} > HI_{uw} \\
\frac{HI_{uw} + HI_{uw} + HI_{uw}}{3} & \text{Otherwise}
\end{cases}$$

where $P_{HI}, HI_{uw}, HI_{uw}, HI_{uw} \in [0, 1]$.

Equation (3) indicates that there are four possible conditions: (1) When $P_{HI} = 0$, it means none of the extracted main watermark and sub-watermark belongs to the target owner (i.e., the property belongs to another owner as both watermarks are closely related). (2) When $P_{HI} = HI_{uw}$, it indicates that the extracted sub-watermark is approximately more intact in comparison with the extracted main watermark (i.e., the property belongs to the target owner with the probability of $P_{HI} = HI_{uw}$). (3) When $P_{HI} = HI_{uw}$, it can be interpreted that the extracted main watermark is approximately more intact in comparison with the extracted sub-watermark (i.e., the property belongs to the target owner with the probability of $P_{HI} = HI_{uw}$). (4) When $P_{HI} = \frac{HI_{uw} + HI_{uw} + HI_{uw}}{3}$, it means the property belongs to the target owner with the probability of $P_{HI} = \frac{HI_{uw} + HI_{uw} + HI_{uw}}{3}$.

Here, if the watermarking approach uses $n$ copies of the same watermarks, then in order to find the best ownership probability, the optimal value of $P_{HI}$ is equal to $f_{Opt}(P_{HI_1}, P_{HI_2}$,
\( \ldots, P_{H_{I_n}} \) such that it can be described as Equation (4).

\[
\begin{align*}
    f_{O_p}(P_{H_1}, \ldots, P_{H_n}) &= \begin{cases} 
        P_{H_1} & \text{if } \text{TheSequenceIsSingleton} \\
        f_{O_p}(P_{H_2}, P_{H_1}, P_{H_4}, \ldots) & \text{if } P_{H_1} \leq P_{H_2} \\
        f_{O_p}(P_{H_1}, P_{H_3}, P_{H_4}, \ldots) & \text{Otherwise}
    \end{cases}
\end{align*}
\]  

(4)

3.2. Mathematical Modelling. Let us assume that \( I \) is the original 8-bit gray-scale host image, and \( X_I \) and \( Y_I \) are the height and width of the \( I \) respectively. So the size of \( I \) is \( |I| = X_I \times Y_I \) and image \( I \) can be represented as \( I = \{ \forall P_{ij} \mid 0 \leq i \leq X_I, 0 \leq j \leq Y_I \} \), where \( P_{ij} \in \{ 0, 1, \ldots, 255 \} \). If \( W \) is the watermark that is to be embedded within \( I \), and \( X_w \) and \( Y_w \) are the height and width of \( W \) respectively, the size of \( W \) is \( |W| = X_w \times Y_w \) and \( W \) can be represented as \( W = \{ \forall W_{ij} \mid 0 \leq i \leq X_w, 0 \leq j \leq Y_w \} \) where \( W_{ij} \in \{ 0, 1, \ldots, 255 \} \). But as the watermark \( W \) is normally used as a bit stream, so if \( W_S \) notifies the bit stream of \( W \) then the size of \( W_S \) is \( |W_S| = 8 \times X_w \times Y_w \) in an 8-bit gray-scale watermark image in which each pixel is comprised of eight bits. Now, let \( W_P \) denote the set of none overlapping sub-bit-streams of \( W_S \) such that the length of each sub-bit-stream is equal to \( \beta \). Thus, \( W_P \) can be represented as \( W_P = \{ \forall (b_i b_{i+1} b_{i+2} \ldots b_r) \mid \text{mod} (i, \beta) = 0, \text{mod} (r, \beta) = \beta - 1 \} \) where \( b_i \in \{ 0, 1 \} \), and \( i, r \in [0, |W_S| - 1] \). The size of \( W_P \) is \( |W_P| = \left\lfloor \frac{|W_S|}{\beta} \right\rfloor \). Consequently, the watermark bit stream \( W_S \) can be represented by binary bit-patterns (Table 1) in \( W_P \).

Now let us assume that random variables \( x_n, y_n \) and \( z_n \) denote the number of the sub-bit-streams that are equal to the \( \eta \)th bit-pattern in the original, the extracted, and the computed watermark bit streams respectively. By using these components, bit-pattern histograms: \( H_u(u), H_v(v) \) and \( H_w(w) \) are formed, where discrete random variables \( u (u \geq 0), v (v \geq 0) \) and \( w (w \geq 0) \) are the observations of the bit-patterns such that \( u, v \) and \( w \) take \( x_n, y_n \) and \( z_n \) values respectively, so

\[
    u = \{x_0, x_1, \ldots, x_n, \ldots, x_L\}
\]

(5)

\[
    v = \{y_0, y_1, \ldots, y_n, \ldots, y_L\}
\]

(6)

\[
    w = \{z_0, z_1, \ldots, z_n, \ldots, z_L\}
\]

(7)

where \( L = 2^\beta - 1 \).

Forming histograms \( H_u(u), H_v(v) \) and \( H_w(w) \) result in ordered sets of discrete values \( \{H_u(x_0), H_u(x_1), \ldots, H_u(x_L)\}, \{H_v(y_0), H_v(y_1), \ldots, H_v(y_L)\} \) and \( \{H_w(z_0), H_w(z_1), \ldots, H_w(z_L)\} \) respectively. In general, the histograms must be normalized. So, let \( P_u(u), P_v(v) \) and \( P_w(w) \) notify the normalized form of histograms \( H_u(u), H_v(v) \) and \( H_w(w) \) in expressions (8), (9) and (10) respectively.

\[
    P_u(u) = \frac{H_u(u)}{|W_P|} = \left\{ \frac{H_u(x_0)}{|W_P|}, \frac{H_u(x_1)}{|W_P|}, \ldots, \frac{H_u(x_L)}{|W_P|} \right\} 
\]

(8)

\[
    P_v(v) = \frac{H_v(v)}{|W_P|} = \left\{ \frac{H_v(y_0)}{|W_P|}, \frac{H_v(y_1)}{|W_P|}, \ldots, \frac{H_v(y_L)}{|W_P|} \right\} 
\]

(9)

\[
    P_w(w) = \frac{H_w(w)}{|W_P|} = \left\{ \frac{H_w(z_0)}{|W_P|}, \frac{H_w(z_1)}{|W_P|}, \ldots, \frac{H_w(z_L)}{|W_P|} \right\} 
\]

(10)

In fact, \( P_u(u), P_v(v) \) and \( P_w(w) \) are the normalized representations of the number of bit-pattern observations in \( H_u(u), H_v(v) \) and \( H_w(w) \) respectively. Hence, the summation
of all components in each of $P_u(u)$, $P_v(v)$ and $P_w(w)$ must be 1 as expressions (11), (12) and (13) show.

\[
\sum_{i=0}^{L} P_u(x_i) = \frac{1}{|W_P|} \sum_{i=0}^{L} H_u(x_i) = 1
\]  
\[
\sum_{i=0}^{L} P_v(y_i) = \frac{1}{|W_P|} \sum_{i=0}^{L} H_v(y_i) = 1
\]  
\[
\sum_{i=0}^{L} P_w(z_i) = \frac{1}{|W_P|} \sum_{i=0}^{L} H_w(z_i) = 1
\]  

Now let the corresponding cumulative distributions $T_u(k)$, $T_v(m)$ and $T_w(n)$ associated with three histograms $H_u(u)$, $H_v(v)$ and $H_w(w)$ be as expressions (14), (15) and (16).

\[
T_u(k) = \sum_{i=0}^{k} H_u(x_i), \quad k = 0, 1, \ldots, L
\]  
\[
T_v(m) = \sum_{i=0}^{k} H_v(y_i), \quad m = 0, 1, \ldots, L
\]  
\[
T_w(n) = \sum_{i=0}^{k} H_w(z_i), \quad n = 0, 1, \ldots, L
\]  

If the size of attacked image is equal to the size of the host image then

\[
T_u(k) = T_v(m) = T_w(n) = \frac{|W_s|}{\beta}
\]  

With the aim of identifying the ownership of an attacked image approximately, we used $HI$ technique given in Equation (2). This technique was utilized to evaluate the similarity rate between each pair of the mentioned histograms. Hence, $HI_{uv}$, $HI_{uw}$, $HI_{vw}$ can be represented as Equations (18), (19) and (20) respectively.

\[
HI_{uv} = \sum_{i=0}^{L} \min(P_u(x_i), P_v(y_i))
\]  
\[
HI_{uw} = \sum_{i=0}^{L} \min(P_u(x_i), P_w(z_i))
\]  
\[
HI_{vw} = \sum_{i=0}^{L} \min(P_v(y_i), P_w(z_i))
\]  

Now the probability of ownership using Equation (3) can be represented as Equation (21).

\[
P(Ownership) = P_{HI}(HI_{uv}, HI_{uw}, HI_{vw})
\]  

Here, if several copies of the same watermarks are used then the $P_{Optimal}(Ownership)$ using Equation (4) can be represented as Equation (22),

\[
P_{Optimal}(Ownership) = f_{Opt}(P_{HI_1}, P_{HI_2}, \ldots, P_{HI_i}, \ldots, P_{HI_n}); \quad i \in \{1, 2, \ldots, n\}
\]
where \( n \) is the number of copies of the same watermark.

4. Experimental Results and Discussions. Results of the experimental investigations based on the proposed scheme were achieved. Description, analysis and discussions of these studies are presented in the following subsections.

4.1. Description. The 8-bit gray-scale standard “Lena” with the size of 512 \( \times \) 512 pixels was chosen in the experiment. Several smooth areas of this famous image make it suitable to obtain appropriate results. Here, two types of watermark have been considered as a watermark-pair. The main watermark was an arbitrary logo of 38 \( \times \) 89 pixels as the main watermark, and the sub-watermark, which delivered the statistical information regarding the main watermark, was in the form of bit-pattern histogram. Nine copies of this watermark-pair were embedded within the host image and indexed with 1 to 9.

The results of the experiments were obtained when the \( HI \) technique was used for BII-LSB approach under JPEG2000, Cropping (30\%) and Reset Removal (60\%) attacks when the bit-pattern lengths (\( \beta \)) were \( \beta = 2, \beta = 3, \beta = 4 \) and \( \beta = 5 \). In order to simulate the watermarking attacks, Adobe Photoshop CS5, JPEG2000 Compressor, and Matlab R2010 built-in functions were used. The JPEG2000 lossy compression attack was used after the embedding stage. The JPEG2000 attack reduced the size of Lena image from 263,222 bytes to 36,083 bytes. Here, in order to embed the main watermark and the sub-watermark, the 2nd and 5th bit-planes (\( HP = 2 \) and \( WP = 5 \)) were used respectively. In each step of the embedding process, the nearest value to the current pixel value which delivered the embedding watermark bit was obtained.

With the aim of evaluating the robustness of the watermarking algorithm, the BCR (Bit Correct Ratio) metric [20,21] was used. With the purpose of evaluating the imperceptibility of watermarked image, the PSNR (Peak Signal to Noise Ratio) metric has been widely used by many researchers [2,5,11,20,21,23-27,30]. In our experiments, PSNR was used to assess the visual imperceptibility.

4.2. Analysis of the results. Table 2, Table 3, Table 4 and Table 5 show the results of the experiments using the proposed scheme after JPEG2000 lossy compression attack when \( \beta = 5, \beta = 4, \beta = 3 \) and \( \beta = 2 \) respectively. These tables show that the probability of the ownership has taken values of 0.48, 0.53, 0.85 and 0.93 when \( \beta = 5, \beta = 4, \beta = 3 \) and \( \beta = 2 \) respectively. These results revealed that the level of the proposed approximation approach inversely changed when \( \beta \) varied. This means if \( \beta = 2 \), with a great probability the ownership of the attacked watermarked image can be well identified. Therefore, the proposed approach was quite robust against JPEG2000 lossy compression attack when \( \beta = 2 \).

Figure 5 shows the watermarked image before and after JPEG2000 lossy compression attack when \( \beta = 2 \). This figure obviously shows that the extracted main watermark can no longer be used for the ownership identification of the property as it was totally corrupted. However, the statistical information regarding the remaining information was intact and was able to be applied by the proposed scheme for the ownership identification of the attacked watermarked image. In other words, the remaining information in both the computed histogram 5(e) and the sub-watermark 5(d) delivered some statistical information about the original histogram 5(c) regarding the embedded main watermarks which could be utilized for the ownership identification of the property. The results of the mentioned experiments can be shown graphically in Figure 6.

Figure 7 shows the results of the PSNR values using the proposed scheme with \( \beta \) values ranging from 2 to 5. This figure illustrates that the quality of the watermarked image is higher when \( \beta \) is lower. This could be anticipated as the higher bit-patterns need more
Table 2. Results of experiments under JPEG2000 lossy compression attack when $\beta = 5$

<table>
<thead>
<tr>
<th>Watermark Pair</th>
<th>$HI_{uv}$</th>
<th>$HI_{uw}$</th>
<th>$HI_{uw}$</th>
<th>$PHI$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.2470</td>
<td>0.5184</td>
<td>0.6005</td>
<td>0.4553</td>
</tr>
<tr>
<td>2</td>
<td>0.3587</td>
<td>0.4179</td>
<td>0.5962</td>
<td>0.4576</td>
</tr>
<tr>
<td>3</td>
<td>0.2821</td>
<td>0.4012</td>
<td>0.5778</td>
<td>0.4204</td>
</tr>
<tr>
<td>4</td>
<td>0.2765</td>
<td>0.4358</td>
<td>0.4916</td>
<td>0.4013</td>
</tr>
<tr>
<td>5</td>
<td>0.2190</td>
<td>0.4179</td>
<td>0.6213</td>
<td>0.4194</td>
</tr>
<tr>
<td>6</td>
<td>0.3623</td>
<td>0.3992</td>
<td>0.5961</td>
<td>0.4525</td>
</tr>
<tr>
<td>7</td>
<td>0.4050</td>
<td>0.4387</td>
<td>0.6044</td>
<td>0.4827</td>
</tr>
<tr>
<td>8</td>
<td>0.3040</td>
<td>0.4040</td>
<td>0.5867</td>
<td>0.4316</td>
</tr>
<tr>
<td>9</td>
<td>0.3024</td>
<td>0.4132</td>
<td>0.6302</td>
<td>0.4486</td>
</tr>
<tr>
<td>$P_{\text{Optimal (Ownership)}}$</td>
<td></td>
<td></td>
<td></td>
<td>0.4827</td>
</tr>
</tbody>
</table>

Table 3. Results of experiments under JPEG2000 lossy compression attack when $\beta = 4$

<table>
<thead>
<tr>
<th>Watermark Pair</th>
<th>$HI_{uv}$</th>
<th>$HI_{uw}$</th>
<th>$HI_{uw}$</th>
<th>$PHI$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.4650</td>
<td>0.5572</td>
<td>0.5782</td>
<td>0.5335</td>
</tr>
<tr>
<td>2</td>
<td>0.3727</td>
<td>0.4438</td>
<td>0.6402</td>
<td>0.4856</td>
</tr>
<tr>
<td>3</td>
<td>0.3149</td>
<td>0.4206</td>
<td>0.5477</td>
<td>0.4278</td>
</tr>
<tr>
<td>4</td>
<td>0.2809</td>
<td>0.4435</td>
<td>0.4449</td>
<td>0.3898</td>
</tr>
<tr>
<td>5</td>
<td>0.3445</td>
<td>0.4446</td>
<td>0.6898</td>
<td>0.4930</td>
</tr>
<tr>
<td>6</td>
<td>0.2787</td>
<td>0.4091</td>
<td>0.6507</td>
<td>0.4462</td>
</tr>
<tr>
<td>7</td>
<td>0.2468</td>
<td>0.4475</td>
<td>0.4493</td>
<td>0.3812</td>
</tr>
<tr>
<td>8</td>
<td>0.2709</td>
<td>0.4163</td>
<td>0.5855</td>
<td>0.4242</td>
</tr>
<tr>
<td>9</td>
<td>0.3768</td>
<td>0.4156</td>
<td>0.5677</td>
<td>0.4534</td>
</tr>
<tr>
<td>$P_{\text{Optimal (Ownership)}}$</td>
<td></td>
<td></td>
<td></td>
<td>0.5335</td>
</tr>
</tbody>
</table>

Table 4. Results of experiments under JPEG2000 lossy compression attack when $\beta = 3$

<table>
<thead>
<tr>
<th>Watermark Pair</th>
<th>$HI_{uv}$</th>
<th>$HI_{uw}$</th>
<th>$HI_{uw}$</th>
<th>$PHI$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.5051</td>
<td>0.8492</td>
<td>0.5746</td>
<td>0.8492</td>
</tr>
<tr>
<td>2</td>
<td>0.3586</td>
<td>0.7426</td>
<td>0.5308</td>
<td>0.7426</td>
</tr>
<tr>
<td>3</td>
<td>0.3982</td>
<td>0.7329</td>
<td>0.6653</td>
<td>0.7329</td>
</tr>
<tr>
<td>4</td>
<td>0.4453</td>
<td>0.7275</td>
<td>0.6181</td>
<td>0.7275</td>
</tr>
<tr>
<td>5</td>
<td>0.2331</td>
<td>0.7331</td>
<td>0.3126</td>
<td>0.7331</td>
</tr>
<tr>
<td>6</td>
<td>0.6612</td>
<td>0.7172</td>
<td>0.6553</td>
<td>0.7172</td>
</tr>
<tr>
<td>7</td>
<td>0.4720</td>
<td>0.7560</td>
<td>0.4896</td>
<td>0.7560</td>
</tr>
<tr>
<td>8</td>
<td>0.6542</td>
<td>0.7206</td>
<td>0.7579</td>
<td>0.7109</td>
</tr>
<tr>
<td>9</td>
<td>0.4112</td>
<td>0.7166</td>
<td>0.6284</td>
<td>0.7166</td>
</tr>
<tr>
<td>$P_{\text{Optimal (Ownership)}}$</td>
<td></td>
<td></td>
<td></td>
<td>0.8492</td>
</tr>
</tbody>
</table>

pixels of the host image. Figure 7 shows that among the tested $\beta$ values, the visual imperceptibility was the highest when $\beta = 2$.

We implemented all EISB-based approaches under Reset Removal, Cropping, and JPEG2000 lossy compression attacks with the same conditions as those in Section 4.1. Table 6 indicates the results of the ownership identification of the attacked watermarked
Figure 5. The results of the experiment after JPEG2000 attack on the proposed scheme. This experiment shows the results of the proposed approach when $\beta = 2$, $WP = 5$ and $HP = 2$, where (a) is the original main watermark, (b) indicates the extracted main watermark (after attack), (c) represents the original sub-watermark, (d) denotes the extracted sub-watermark (after attack), and (e) is the computed sub-watermark (after attack).

Figure 6. Ownership probability results using different $\beta$ values after JPEG2000 attack

Figure 7. PSNR values of the proposed scheme using different $\beta$ values
image in EISB approach using the 3rd bit-plane [29], Biased-EISB technique using the 4th bit-plane when the bias value was 6 [8], EISB approach using L2Norm [45], and the Block-Based Biased-EISB approach using the 4th bit-plane when the Bias value was 6 and the block size was 3 × 3 [43].

Table 6. Robustness comparison between the proposed scheme and other watermarking approaches after attacks (for the robustness, the values in the range of 0.50-0.69, 0.70-0.79, 0.80-1.00 were considered as “LOW”, “MEDIUM”, “HIGH” respectively)

<table>
<thead>
<tr>
<th>Watermarking Approach</th>
<th>EISB Approach 3rd bit-plane</th>
<th>EISB Approach Using L2Norm</th>
<th>Block-Based Biased-EISB 4th bit-plane (Bias value = 6) (Block Size: 3 × 3)</th>
<th>Biased-EISB 4th bit-plane (Bias value = 6)</th>
<th>Proposed Scheme (HP = 2 WP = 5) (β = 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Removal (60%)</td>
<td>HIGH</td>
<td>HIGH</td>
<td>LOW</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Cropping (30%)</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>JPEG2000</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

4.3. Discussions. Table 6 shows the results from the robustness point of view between the proposed scheme and other watermarking approaches after JPEG2000 lossy compression, Cropping (30%) and Reset Removal (60%) attacks. This table illustrates that the robustness of Biased EISB, EISB, EISB using L2Norm, and the proposed approach were high against Reset Removal and Cropping attacks. This could be anticipated because these four approaches employed multi-watermarking strategy. In contrast, in the case of Block-Based Biased-EISB approach because the embedding capacity was low, the multi-watermarking strategy could not be applied so the robustness of this approach was not high against such attacks. Table 6 also illustrates that neither Biased EISB, EISB, nor EISB using L2Norm approaches could withstand against JPEG2000 lossy compression attack. In contrast, both the proposed scheme, and Block-based Biased-EISB approach...
withstood against that attack well. From the perspective of watermarking quality, Table 7 shows the results of the experiments on the five mentioned approaches. According to Istepanian et al. [42], for medical studies and clinical applications the favorable PSNR values are the values of more than 35 dB. Li et al. [44] proposed a minimum value of 40 dB for medical applications. Table 7 illustrates that the quality of Biased EISB, EISB, EISB using L2Norm, and Block-Based Biased-EISB approaches was not high enough for many real-time applications such as photography, medical studies and clinical applications. In actual fact, the Biased technique drastically degraded the watermarked image quality in both Biased EISB and Block-based Biased-EISB approaches. Similarly, in both EISB, and EISB using L2Norm approaches, the use of a high ISB bit-plane resulted in degradation of the watermarked image quality. In contrast, Table 7 obviously shows that the proposed scheme results in high imperceptibility in the watermarked image. In conclusion, the proposed scheme can highly balance the trade-off between imperceptibility and robustness.

Figure 8. Watermarking quality comparison result between the proposed scheme (a) when $\beta = 2$, $WP = 5$, $HP = 2$ and PSNR = 42, and Block-Based Biased-EISB approach, (b) when bit-plane = 4th, Bias value = 6, Block Size= $3 \times 3$ and PSNR = 30

Table 7. Quality comparison between the proposed scheme and other watermarking approaches

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality</td>
<td>30 dB</td>
<td>32 dB</td>
<td>32 dB</td>
<td>30 dB</td>
<td>42 dB</td>
</tr>
<tr>
<td>Effective Capacity</td>
<td>$\leq 12.5%$</td>
<td>$\leq 12.5%$</td>
<td>$\leq 12.5%$</td>
<td>$\leq 1.4%$</td>
<td>$\geq 12.5%$</td>
</tr>
</tbody>
</table>
5. Conclusions and Future Works. This paper proposed a novel approach based on approximation strategy utilizing Histogram Intersection (HI) technique for the ownership identification of the digital watermarked image assets which carry destroyed watermarks. The key idea behind this approach was the use of the remaining information of the attacked watermarked image based on bit-pattern histograms. We implemented and tested the proposed approach against JPEG 2000 lossy compression, Cropping (30%) and Reset Removal (60%) attacks with $\beta$ coefficient ranging from 2 to 5. Here, the most significant results have revealed that the proposed approach preserved significantly the host image quality, and at the same time, successfully identified the rightful owner of the image property using the remaining information of the corrupted watermarks. Thus, the proposed scheme can highly balance the trade-off between imperceptibility and robustness.

For future works, the proposed approach can be utilized in other watermarking approaches including transform domain approaches such as DCT (Discrete Cosine Transform), FFT (Fast Fourrier Transform), DWT (Discrete Wavelet Transform) and HT (Hadamard Transform).

Acknowledgment. This work was supported by UTMVicubelab at Department of Computer Graphics and Multimedia, Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia (UTM), under the Research University Grant Scheme (RUGS) with Reference No. Q.J130000.712S.01J12 for providing financial support of this research. The authors thank UTM for the award of International Doctoral Fellowship (IDF) leading to Mir Shahriar Emami. The authors also gratefully acknowledge the suggestions made by anonymous reviewers that have enhanced greatly the quality of the manuscript.

REFERENCES


