# Multi-party Watermark Embedding with Frequency-Hopping Sequences

Limengnan Zhou

School of Electronic and Information Engineering
University of Electronic Science and Technology of China, Zhongshan Institute
Zhongshan 528400, Guangdong, China

dreamzlmn@foxmail.com

Hanzhou Wu

School of Communication and Information Engineering
Shanghai University
Shanghai 200444, Shanghai, China

h.wu.phd@ieee.org

**Abstract**

In this paper, we introduce a multi-party watermark embedding algorithm based on frequency-hopping sequences (FHSs). In the proposed method, a certain number of FHSs are predetermined and then randomly assigned to multiple parities, who are the co-copyright holders of a digital object. All the parties will use the assigned FHS to insert their own ownership information to the digital object by altering the corresponding elements within the object without impairing its commercial use. In this way, each party can use the assigned FHS to recover the ownership information to verify their own ownership if required. Since the used FHSs can result in a very low number of element collisions, the probability of altering the identical content within the digital object would be low such that the error rate of data extraction for each party will be low. Moreover, if the digital object was modified, the embedded information can be still retrieved to claim the ownership as the FHSs provide high randomness. Experimental results have shown that, our work enables the multiple parties to reliably verify their own ownership even the product was maliciously attacked by common operations, which has verified the superiority and applicability.

## 1 Introduction

The rapid development of the Internet and social networks have brought comprehensive changes to our daily livings, leading many commercial enterprises to move their novel products from offline experience to online consumption. For example, online movie, online music, and online personal photo-sharing are quite popular in social networks nowadays.

While we are benefited from these online services, we are also facing many security issues from the viewpoint of the service providers, among which how to protect the ownership of the digital products is one of the most important yet challenging topic.

Information hiding [1] is such a technique that it allows us to hide a secret message into a digital object (also called *cover*) such as image and video without significantly distorting the object content. The resulting object containing hidden information (also called *marked* object) can be processed to reconstruct the hidden information according to the secret key. Therefore, it is desirable to consider information hiding as a means to protect the ownership, which is typically called digital watermarking [2], [3]. In detail, given a cover to be protected, the content owner first hides secret data into the cover by applying a reliable digital watermarking algorithm without affecting the use of the cover. Then, the resulting marked object will be released for profits or services. When it is necessary to claim the ownership, the content owner has to reconstruct the secret data from the marked object that may be previously attacked, e.g., by random noise. If the content owner can reconstruct the ownership information with a tolerable rate of errors, then the ownership can be protected.

If a digital cover has only one owner, the digital cover can be modified only once. However, in modern business, in order to provide high-quality services, the production of a digital product may need multi-party cooperation. For instance, producing a very high-quality movie video requires many advanced video processing technologies, which, however, may be not mastered by only one company. That means, during the video processing phase, one may ask multiple parties for cooperation such that a high-quality video can be generated at the expense that each party may hold the ownership. Even though some parties may not completely hold the ownership, they may also want to insert additional information into the product so that, the inserted information does not impair the use of the product and it can prove that the parties have contributed to the production of the product, which will be helpful when commercial disputes exist in future. It requires us to embed multiple pieces of ownership information into the product (cover).

Obviously, each party can hide his own information into the cover without considering the actions taken by any other parties. However, it would lead to two problems if the multiple parties embed data into the cover by themselves. The first one is, a party may not successfully extract his own data from the marked version since the embedded data may be overwritten by other parties. This problem is caused by the fact that two independent parties may use the same content to carry the extra data. The second one is, when multiple parties embed extra data into the cover, the introduced distortion may be significant, which may impair the commercial use of the cover.

Therefore, it is necessary to design such a watermarking system that, each party can perfectly/near-perfectly extract his own data from the marked product for ownership verification or other purposes, and the introduced distortion is low so that the use of the product will not be affected. To this end, in this paper, we propose to use frequency-hopping sequences (FHSs) to deal with the aforementioned problem. The main idea is to generate a set of FHSs (hopping pattern) with a very low number of collusions (even no collusion) such that each party can use exactly one sequence from the set to identify the cover elements to be exploited for watermark embedding. In this way, the probability of

using the identical elements for watermark embedding for two parties is extremely low, meaning that, each party can reliably extract his own watermark. Moreover, since the FHSs have good randomness, even the marked content was intentionally modified, the watermark for each party can be still extracted with a low error rate, which has verified by our convinced experiments.

The rest of this paper is organized as follows. In Section 2, we review FHSs. In Section 3, we detail the proposed multi-party watermarking system, followed by performance evaluation and analysis in Section 4. Finally, we conclude this paper in Section 5.

## 2 Frequency-Hopping Sequences

In frequency-hopping multiple-access systems, FHSs are used to decide which frequency we should choose to transmit the information in each time slot. As is often the case, it will come to mutual interference when two or more users transmit information on the same frequency slot at the same time [4, 5, 6]. FHSs also can be applied to the proposed watermarking system. Clearly, in our multi-party watermarking system, the function of FHSs is to decide which cover elements should be selected to carry the secret information. That is to say, the positions of the selected cover elements may hop with the rule of FHSs. When two or more parties use the same position to hide information, it would cause overwriting which is mainly controlled by the Hamming correlations of the employed FHSs. And, overwriting will introduce large distortion if the modification is significant. To reconstruct all watermarks and keep the distortion low, the Hamming correlations between different FHSs should be as small as possible. Furthermore, for each employed FHS, as we may use a part of the sequence instead of the whole sequence, the peroiodic partial Hamming correlations (PPHCs) of FHSs play an important role in reflecting the performance of the proposed watermarking system. Besides, the time delay between different employed FHSs also can be viewed as a secret key to each party. Next, we will introduce basic concepts about PPHCs of FHSs.

Let $F = \{f_0, f_1, ..., f_{r-1}\}$ be a frequency slot set with $r$ available frequency slots, and $\mathbf{H} = \{\mathbf{h}_0, \mathbf{h}_1, ..., \mathbf{h}_{e-1}\}$ be an FHS set with $e$ FHSs of length $g$ over $F$ such that each element of each sequence in $\mathbf{h}$ is in $F$. For any two FHSs $\mathbf{h}_{i_1} = [h_{i_1,0}, h_{i_1,1}, \cdots, h_{i_1,g-1}], \mathbf{h}_{i_2} = [h_{i_2,0}, h_{i_2,1}, \cdots, h_{i_2,g-1}] \in \mathbf{H}, 0 \leq i_1, i_2 < e$, and any correlation window length $W, 1 \leq W \leq g$ starting at $w, 0 \leq w < g$, the PPHC function [7] between $\mathbf{h}_{i_1}$ and $\mathbf{h}_{i_2}$ at time delay $\tau$ is defined as follows:

$$T_{\mathbf{h}_{i_1},\mathbf{h}_{i_2}}(w|W;\tau) = \sum_{x=w}^{w+W-1} t(h_{i_1,x}, h_{i_2,x+\tau}),$$

where $t(h_{i_1,x}, h_{i_2,x+\tau}) = 1$ if $h_{i_1,x} = h_{i_2,x+\tau}$, and 0 otherwise. In addition, all the operations among the position indices are performed modulo $g$. $T_{\mathbf{h}_{i_1},\mathbf{h}_{i_2}}(w|W;\tau)$ is called as the periodic partial Hamming autocorrelation function if $i_1 = i_2$, and called as the periodic partial Hamming cross-correlation otherwise.

The maximum periodic partial Hamming autocorrelation $T_{pam}(\mathbf{H}; W)$, maximum periodic partial Hamming cross-correlation $T_{pcm}(\mathbf{H}; W)$, and maximum PPHC $T_{pm}(\mathbf{H}; W)$

of $\mathbf{H}$ are respectively defined as:

$$\begin{aligned}
&T_{pm}(\mathbf{H};W) = \max\{T_{pam}(\mathbf{H};W), T_{pcm}(\mathbf{H};W)\},\\
&T_{pam}(\mathbf{H};W) = \max_{0\le i<e, 1\le\tau<g, 0\le W<g}\{T_{s_i,s_i}(w|W;\tau)\},\\
&T_{pcm}(\mathbf{H};W) = \max_{0\le i\ne j<e, 0\le\tau,w<g}\{T_{s_i,s_j}(w|W;\tau)\}.
\end{aligned}$$

$T_{pm}(\mathbf{H};W)$ is also called as the maximum periodic Hamming correlation (PHC) of $\mathbf{H}$ and denoted as $T_m(\mathbf{H})$ if $W = g$.

Practically, the time delay betweent each party maybe restricted in a zone around the origin, we can use FHSs with low-hit-zone (LHZ) in the proposed watermarking system. For any FHS set $\mathbf{H}$ and correlation window length $W$ starting at $w$, let integers $T_{paz}, T_{pcz} > 0$. Then, the periodic partial Hamming autocorrelation low-hit-zone (LHZ) $L_{paz}$, the periodic partial Hamming cross-correlation LHZ $L_{pcz}$, the PPHC-LHZ $L_{pz}$, and the maximum PPHC $T_{pzm}(\mathbf{H};W)$ within the LHZ of $\mathbf{H}$ [8, 9] are respectively defined as:

$$\begin{aligned}
&L_{paz} = \max\{Z|T_{\mathbf{h}_{i_1},\mathbf{h}_{i_1}}(w|W;\tau) \le T_{paz}:\ 0<\tau\le Z,\ 0\le w<g, 0\le i_1<e\},\\
&L_{pcz} = \max\{Z|T_{\mathbf{h}_{i_1},\mathbf{h}_{i_2}}(w|W;\tau) \le T_{pcz}:\ 0\le\tau\le Z,\ \ 0\le w<g, 0\le i_1\ne i_2<e\},\\
&L_{pz} = \min\{L_{paz}, L_{pcz}\},\\
&T_{pzm}(\mathbf{H};W) = \max\{T_{paz}, T_{pcz}\}.
\end{aligned}$$

Specially, $T_{pzm}(\mathbf{H};W)$ is also called as the maximum PHC within the LHZ of $\mathbf{H}$ and can be denoted as $T_{zm}(\mathbf{H})$ if $W = g$.

For simplicity, we denote an LHZ-FHS set consisting of $e$ FHSs with length $g$ over frequency slot set $F$ sized $r$ and having maximum PPHC $T_{pzm}(\mathbf{H};W)$ within the correlation window length $W$ and LHZ $L_{pz}$ as an $(g, e, r, W, L_{pz}, T_{pzm}(\mathbf{H};W))$ LHZ-FHS set.

We next choose Liu's LHZ-FHS set $\mathbf{H}$ in [10] as an example for better explanation. Let $p$ be a prime number, $\mathbf{F}_p$ and $\mathbf{F}_{p^n}, n>1$ be the finite field of order $p$ and $p^n$ respectively, and $\eta$ be the primitive element of $\mathbf{F}_{p^n}$. It is obviously that $(\mathbf{F}_p, +)$ is a subgroup of $(\mathbf{F}_{p^n}, +)$. Thus, there exist $p^{n-1}$ elements $m_0, m_1, \cdots, m_{p^{n-1}-1}$ in $\mathbf{F}_{p^n}$ such that

$$CS_i = m_i + \mathbf{F}_p = \{m_i + \beta, \beta\in\mathbf{F}_p\}\ ,\ 0\le i<p^{n-1}$$

are just the $p^{n-1}$ cosets of $\mathbf{F}_p$ in $\mathbf{F}_{p^n}$. That is to say,

$$\mathbf{F}_{p^n} = \bigcup_{i=0}^{p^{n-1}-1} CS_i$$

and

$$CS_i \bigcap CS_j = \emptyset\ ,\ 0\le i\ne j<p^{n-1}.$$

**Lemma 1** ([10]: Liu's FHS set)**.** *With the notations as above, a* $(p(p^n-1), p^n, p^n, W, p^n-2, \left\lceil\frac{W}{p^n-1}\right\rceil)$ *FHS set* $\boldsymbol{H} = \{\boldsymbol{h}_i, 0\le i<p^n\}$ *over* $\boldsymbol{F}_{p^n}$ *can be expressed as:*

$$\boldsymbol{h}_{i,x} = a_i + \eta^{\langle x\rangle_{p^n-1}} + \langle x\rangle_p\,, \tag{1}$$

*where* $a_i\in CS_i, 0\le i<p^n$.

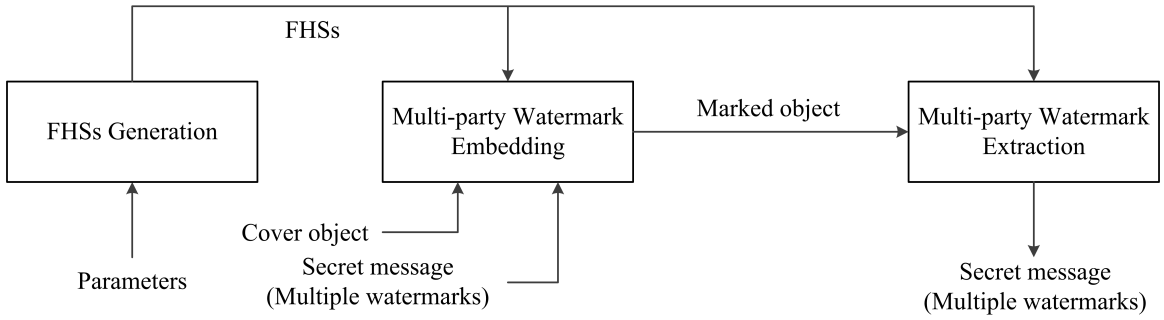


Figure 1: Sketch for the proposed multi-party watermarking system.

**Example 2.** Let $p = 2$, $n = 9$, and $\eta$ be the primitive element of the finite field $\mathbf{F}_{2^9}$ with $\eta^9 = \eta^4 + 1$. For simplicity, we denote $\eta^i, 0 \le i \le 510$, as $i$ and 0 as 511. Then, we can have a Liu's LHZ-FHS set $\mathbf{H}$ as:

$$\begin{aligned}
\mathbf{h}_0 &= [0, 130, 2, 420, 4, 507, 6, 67, 8, 4, 10, 470, 12, 138, 14, 126, 16, 341, 18, 421, 20, \\
&\quad \cdots, 495, 111, 497, 125, 499, 459, 501, 506, 503, 60, 505, 502, 507, 417, 509, 129], \\
\mathbf{h}_1 &= [511, 1, 260, 3, 9, 5, 329, 7, 18, 9, 503, 11, 147, 13, 134, 15, 36, 17, 8, 19, 495, 21, \\
&\quad \cdots, 494, 20, 496, 120, 498, 135, 500, 493, 502, 10, 504, 323, 506, 5, 508, 258, 510], \\
&\vdots \\
\mathbf{h}_{511} &= [129, 289, 419, 18, 506, 416, 66, 341, 3, 506, 469, 438, 137, 332, 125, 231, 340, \\
&\quad \cdots, 323, 421, 110, 49, 124, 14, 458, 402, 505, 4, 59, 166, 501, 9, 416, 210, 128, 0].
\end{aligned}$$

For any $0 < \tau \le 510$ if $0 \le i_1 = i_2 < 511$, and for any $0 \le \tau \le 510$ if $0 \le i_1 \ne i_2 < 511$, and the correlation window length $W, 1 \le W \le 1022$, starting at $w, 0 \le w < 1022$, we always have

$$T_{\mathbf{h}_{i_1}, \mathbf{h}_{i_2}}(w|W;\tau) \le \left\lceil \frac{W}{511} \right\rceil.$$

Therefore, $\mathbf{H}$ is a $(1022, 512, 512, W, 510, \left\lceil \frac{W}{511} \right\rceil)$ LHZ-FHS set.

## 3 Proposed Multi-party Watermarking System

In this section, we introduce the proposed multi-party watermarking system in detail. As shown in Fig. 1, the system design consists of three modules, i.e., FHSs generation, multi-party watermark embedding, and multi-party watermark extraction. The target of FHSs generation is to produce a number of FHSs based on the predetermined parameters. The generated FHSs will be assigned to the co-copyright holders. For multi-party watermark embedding, it allows the co-copyright holders to cooperatively generate a marked version of the cover, which will be released for use. Finally, the multi-party watermark extraction

aims to reconstruct the embedded watermarks from the marked object that was probably previously altered for ownership verification.

Without the loss of the generalization, we model the cover object as an integer sequence and let $\mathbf{c} = \{c_1, c_2, ..., c_n\}$ denote the cover sequence sized $n > 0$, where $c_i, 1 \leq i \leq n$, is a non-negative integer representing the $i$-th cover element whose value is $c_i$. The co-copyright holders are denoted by $\{U_1, U_2, ..., U_m\}, m \geq 2$. The secret message to be embedded (i.e., watermark) for $U_i$ is represented by $\mathbf{w}_i \in \{0,1\}^{|\mathbf{w}_i|}$. For the sake of simplicity, we assume that the watermark lengths equal each other, i.e., $|\mathbf{w}_1| = |\mathbf{w}_2| = ... = |\mathbf{w}_m| = l$. Our target is to embed all the watermarks into $\mathbf{c}$ to generate a new sequence $\mathbf{s} = \{s_1, s_2, ..., s_n\}$ (called marked sequence) such that, we can extract a set of watermarks $\{\mathbf{w}'_i | 1 \leq i \leq m\}$ from $\mathbf{s}$ that the distortion between $\mathbf{w}_i$ and $\mathbf{w}'_i$, denoted by $d(\mathbf{w}_i, \mathbf{w}'_i)$, is low for all $1 \leq i \leq m$. As the watermarks are binary streams, the distortion measure can be defined as the Hamming distance in default.

The FHSs generation is completed by the authentication center (a trusted manager), who aims to produce an FHS set including a total of $m$ sequences $\{\mathbf{h}_1, \mathbf{h}_2, ..., \mathbf{h}_m\}$, for which $\mathbf{h}_i = \{h_{i,1}, h_{i,2}, ..., h_{i,n_i}\}$ will be assigned to $U_i$ for all $1 \leq i \leq m$. One may think that $n_1 = n_2 = ... = n_m = l$ for simplicity. It is further required that, for each $U_i, 1 \leq i \leq m$, we always have $0 \leq h_{i,j} \leq \lfloor n/l \rfloor$. The watermark embedding includes three steps. First of all, the cover sequence $\mathbf{c}$ is divided into $l+1$ disjoint sub-sequences $\{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_{l+1}\}$, where $|\mathbf{c}_1| = |\mathbf{c}_2| = ... = |\mathbf{c}_l| = \lfloor n/l \rfloor$ and $|\mathbf{c}_{l+1}| = n - l \cdot \lfloor n/l \rfloor$. Then, only $\{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_l\}$ will be used to carry the $m$ watermarks and $\mathbf{c}_{l+1}$ is unchanged. For each co-copyright holder $U_i, 1 \leq i \leq m$, he should embed $\mathbf{w}_i$ into $\mathbf{c}$ in such a way that each sub-sequence in $\{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_l\}$ carries only one bit in $\mathbf{w}_i$. As the number of used sub-sequences equals $l$, $\mathbf{w}_i$ can be fully embedded.

It is open to design the data embedding operation. For simplicity, we use the least significant bit (LSB) replacement to embed a watermark bit. Clearly, for an integer $x \geq 0$ and a secret bit $b \in \{0,1\}$, the data embedding operation of using LSB replacement can be expressed as: $y = x - (x \bmod 2) + b$, where "mod" means the modulo operation and $y$ represents the marked integer. For example, if $x = 13$ and $b = 0$, then the marked integer is $y = 12$. Therefore, for each $b_j \in \mathbf{w}_i$ to be embedded, the co-copyright holder $U_i$ can use LSB replacement to embed $b_j$ to the $h_{i,j}$-th element of $\mathbf{c}_j$, denoted by $c_{j,h_{i,j}}$, namely,

$$c^{(i)}_{j,h_{i,j}} = c_{j,h_{i,j}} - (c_{j,h_{i,j}} \bmod 2) + b_j, \forall 1 \leq j \leq l.$$

In this way, each $U_i$ can embed $\mathbf{w}_i$ into $\mathbf{c}$ independently, resulting in the corresponding marked sequence, denoted by $\mathbf{c}^{(i)}$. It can be easily inferred that, for any $\mathbf{c}^{(i)} = \{c^{(i)}_1, c^{(i)}_2, ..., c^{(i)}_n\}$ and $\mathbf{c}^{(j)} = \{c^{(j)}_1, c^{(j)}_2, ..., c^{(j)}_n\}$,

$$\lfloor c^{(i)}_k / 2 \rfloor = \lfloor c^{(j)}_k / 2 \rfloor = \lfloor c_k / 2 \rfloor, \forall 1 \leq k \leq n.$$

Finally, the marked sequence $\mathbf{s} = \{s_1, s_2, ..., s_n\}$ can be generated as:

$$s_i = 2 \cdot \lfloor c_i / 2 \rfloor + \left( \sum_{j=1}^{m} c^{(j)}_i \bmod 2 \right), \forall c_i \in \mathbf{c} \setminus \mathbf{c}_{l+1},$$

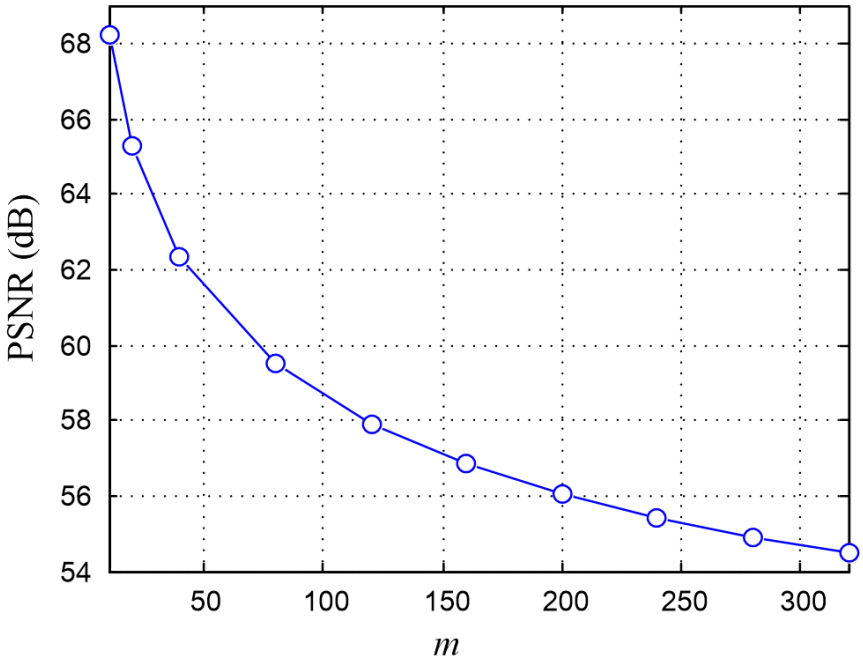


Figure 2: The PSNRs (dB) between $\mathbf{c}$ and $\mathbf{s}$ due to different $m$.

and

$$s_i = c_i, \forall c_i \in \mathbf{c}_{l+1}.$$

$\mathbf{s}$ will be released for use. For watermark reconstruction, $\mathbf{s}$ will be divided into disjoint sub-sequences in the similar way to $\mathbf{c}$. Let $\{\mathbf{s}_1, \mathbf{s}_2, ..., \mathbf{s}_{l+1}\}$ represent the corresponding sub-sequences, where $|\mathbf{s}_1| = |\mathbf{s}_2| = ... = |\mathbf{s}_l| = \lfloor n/l \rfloor$ and $|\mathbf{s}_{l+1}| = n - l \cdot \lfloor n/l \rfloor$. For each $U_i$, he has to reconstruct a watermark $\mathbf{w}_i'$, which should be quite close to $\mathbf{w}_i$ for ownership verification. To this end, $U_i$ has to first use $\mathbf{h}_i$ to identify the embedded elements and then extract all embedded bits. In detail, the $j$-th bit $b_j'$ in $\mathbf{w}_i'$ is determined by:

$$b_j' = s_{j,h_{i,j}} \bmod 2, \forall 1 \leq j \leq l,$$

where $s_{j,h_{i,j}}$ means the $h_{i,j}$-th element in $\mathbf{s}_j$. On the one hand, the LSB replacement ensures that the overall distortion can be kept low even a cover element can be overwritten multiple times. On the other hand, since the FHS set has a very low number of collisions, the number of overwritten cover elements will be small, indicating that, the reconstructed watermark for each $U_i$ will have a small distance to the original one, which can verify the ownership. In addition, since the FHS set also provides good randomness, even $\mathbf{s}$ was attacked, the reconstructed watermarks would still have a low error bit as long as the attack degree was not significant, meaning that, the ownership can be still verified. Here, the assumption that the attack degree was not significant is reasonable since a large attack degree will impair the use of the cover.

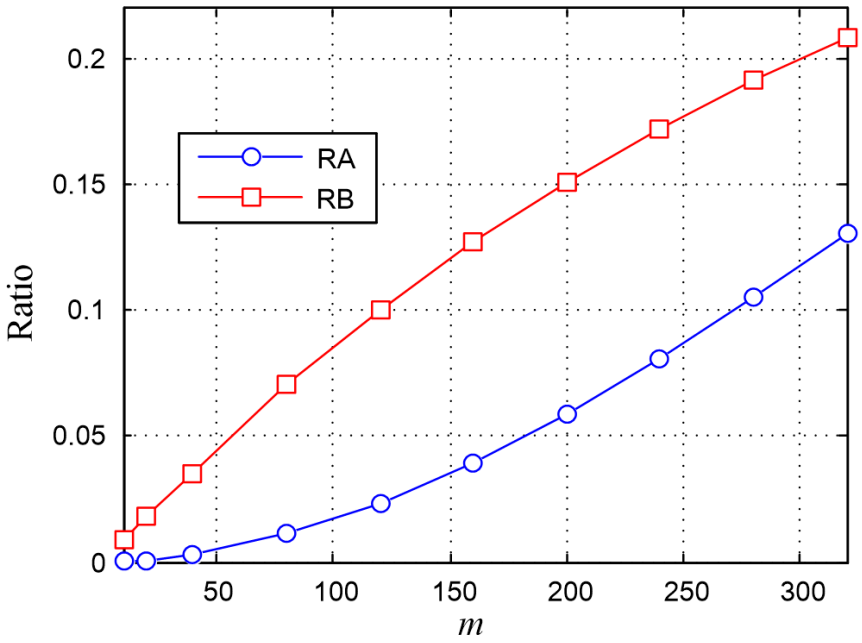


Figure 3: The two ratio curves for collision analysis. RA: the ratio between the number of pixels embedded with at least two times and the number of all pixels in $\mathbf{c}$, RB: the ratio between the number of pixels embedded with at least two times and the sum of the sizes of all watermarks.

## 4 Performance Evaluation and Analysis

In this section, we provide simulation results for evaluation and analysis. We use the standard grayscale image *Lena* sized $512 \times 512$ as the cover. Each pixel is represented with 8 bits, resulting in a pixel value ranging from 0 to 255. All watermarks are considered as a random bit stream. The length of a watermark is set to 512 in default. And, the Liu's LHZ-FHS set $\mathbf{H}$ [10] mentioned in Section II is used to generate the required sequences, i.e., the number of co-copyright holders is in range $[2, 512]$. It is mentioned that, the time delay between any two sequences in the FHS set is restricted in range $[0, 510]$, and the starting point can be realized by random.

We first evaluate the imperceptibility due to watermark embedding. We use peak signal-to-noise ratio (PSNR, dB), which is a common measure used in image quality assessment, to evaluate the visual difference between $\mathbf{s}$ and $\mathbf{c}$. The PSNR is defined as:

$$\mathrm{PSNR} = 10 \cdot \log_{10} \frac{255^2}{\mathrm{MSE}},$$

where

$$\mathrm{MSE} = ||\mathbf{c} - \mathbf{s}||_2^2 / n = \sum_{i=1}^{n} |c_i - s_i|^2 / n.$$

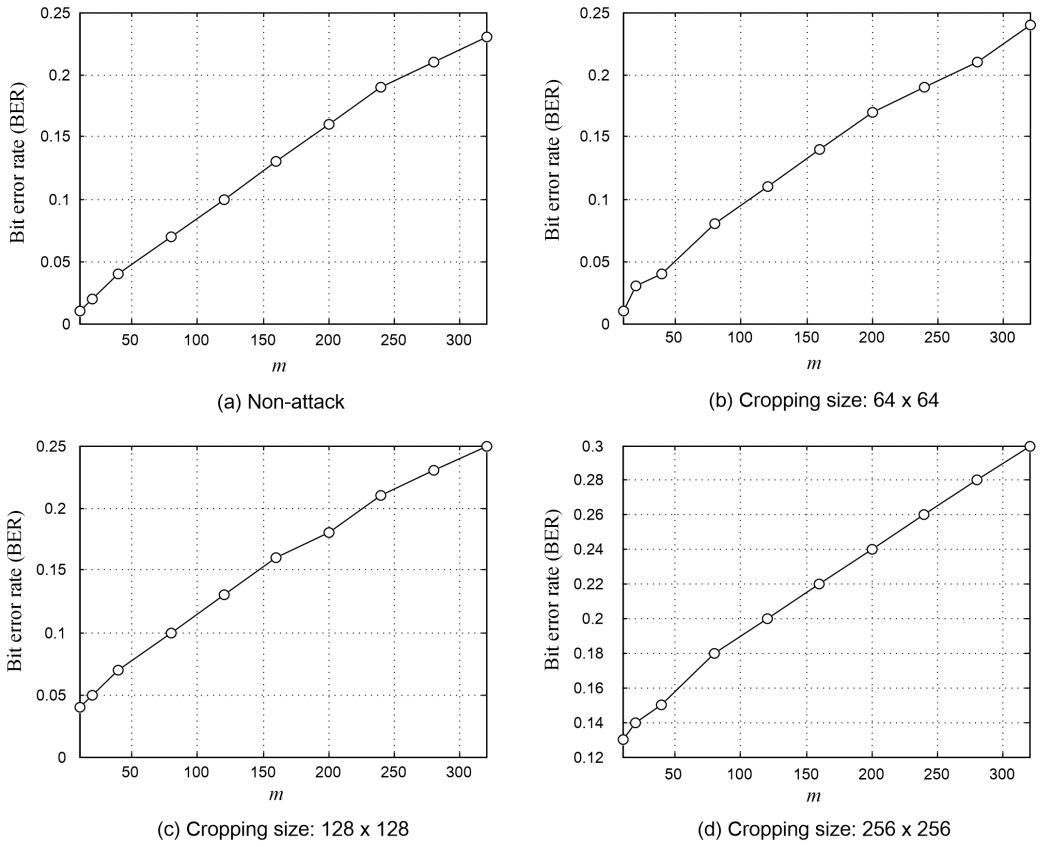


Figure 4: The mean BERs for the extracted watermarks due to different $m$.

Fig. 2 shows the PSNRs due to different $m$. In general, a higher PSNR value corresponds to the better image quality, accordingly well preserving the imperceptibility. It can be observed from Fig. 2 that, as the number of co-copyright holders increases, the image quality will decline since more data were embedded. However, the degradation degree declines smoothly when $m$ increases and all PSNR values are kept with a high level, indicating that, the proposed watermarking system does not impair the imperceptibility.

To analyze the collision, we collect the pixels that were used for data embedding with at least two times. We compute two ratios. The first one is the ratio between the number of pixels embedded with at least two times and the number of all pixels in $\mathbf{c}$. The second one is the ratio between the number of pixels embedded with at least two times and the sum of the sizes of all watermarks. Fig. 3 shows the results. It can be seen that, as $m$ increases, the ratio values for both curves will increase. The reason is that, a larger $m$ means that more sequences are used, which will obviously increase the collisions. However, both curves increase smoothly, indicating that, using the FHS set will not significantly increase the collision probability, which implies that, the watermarks can be all reliably extracted with a low error rate to verify the ownership.

We further evaluate the robustness of the proposed work. Fig. 4 (a) shows the mean bit error rates (BERs) for the extracted watermarks due to different $m$. The mean BER for a fixed $m$ is determined as follows. We first determine the ratio of error bits for each

co-copyright holder. By averaging all ratios, we can then obtain the mean value. It can be observed that, though the mean BER values will increase as $m$ increases, they are all lower than 25%. It shows that, by using FHS, the BER can be kept low. Moreover, it is seen that, for $m \leq 50$, the mean BERs are lower than 5%, meaning that, all watermarks can be extracted with a very low error, which allows each co-copyright holder to successfully claim the ownership. In addition, in applications, the marked object may be attacked, e.g., one may alter the marked content to remove the embedded watermark. To this end, we mimic a common attack. We randomly crop the marked image with a fixed size. Then, we determine the mean BERs. For example, Fig. 4 (b) is corresponding to the case that we randomly crop $\mathbf{s}$ with a pixel block sized $64 \times 64$, i.e., the $64 \times 64$ pixel block is removed. It can be seen from Fig. 4 (b, c, d) that, when the cropping size is smaller, the BERs can be kept lower, which is obvious. When the cropping size is $64 \times 64$, the performance is almost the same as the non-attacked case as shown in Fig. 4 (a). And, even the cropping size is $256 \times 256$ (meaning that, 25% pixels are attacked), the BERs can be still kept relatively low. It indicates that, the FHS has the good ability to resist against cropping attack, which is quite desirable for practice.

## 5 Conclusion and Discussion

In this paper, we make the attempt of applying the FHSs to the design of a multi-party watermarking system. In the work, all parties use an assigned FHS to embed a watermark into the host by altering the corresponding elements. Since the FHS set has a very low number of collisions, the probability of altering the identical content for the multiple parties will be low. Moreover, by using the FHSs, the selected elements to be modified are randomly distributed in the host. Accordingly, each party can use the assigned FHS to recover the watermark with a low distortion to verify the ownership if necessary. Experimental results have shown that, even the marked object was attacked, the watermarks can be still reliably extracted with a low error rate, which enables the multiple parties to reliably verify the ownership. In our experiments, we use the LSB replacement as the data embedding operation, which does not take into account the characteristics of the host itself. In the future, we will combine the FHSs and adaptive data embedding operation so as to further improve the robustness and also enhance the embedding capacity.

## Acknowledgement

This work was partly supported by the National Natural Science Foundation of China under Grant Nos. 61901096 and 61902235, the High Level Talent Research Starting Project in University of Electronic Science and Technology of China, Zhongshan Institute, under Grant No. 417YKQ06, the Sixth Zhongshan Innovation Team Programme – Flexible Internet of Things Enabled by Wireless Energy Transfer under Contract No. 180809162197874, and the Shanghai "Chen Guang" Project under Grant No. 19CG46.

## References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey", *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*, Morgan Kaufmann, 2nd Edition, Nov. 2007.

[3] D. Eppstein, M. T. Goodrich, J. Lam, N. Mamano, M. Mitzenmacher, and M. Torr, "Models and algorithms for graph watermarking," *International Conference on Information Security*, pp 283-301, Aug. 2016.

[4] P. Fan, and M. Darnell, *Sequence design for communications applications*, Research Studies Press (RSP), Wiley, London, 1996.

[5] D. Peng, and P. Fan, "Lower bounds on the hamming auto- and cross correlations of frequency-hopping sequences", *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2149–2154, Sept. 2004.

[6] A. Lempel, and H. Greenberger, "Families of sequences with optimal hamming correlation properties", *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 90–94, Jan. 1974.

[7] X. Niu, D. Peng, F. Liu, and X. Liu, "Lower bounds on the maximum partial correlations of frequency hopping sequence set with low hit zone", *IEICE Trans. Fund.*, vol. E93-A, no.11, pp. 2227–2231, Nov. 2010.

[8] D. Peng, P. Fan, and M. Lee, "Lower bounds on the periodic hamming correlations of frequency hopping sequences with low hit zone", *Sci. China F, Inf. Sci.*, , vol. 49, no. 2, pp. 208–218, Jun. 2006.

[9] L. Zhou, D. Peng, H. Han, H. Liang, and Z. Ma, "Construction of optimal low-hit-zone frequency hopping sequence sets under periodic partial hamming correlation", *Adv. Math. Commun.*, vol.12, no.1, pp. 67–79, Feb. 2018.

[10] X. Liu, and L. Zhou, "New bound on partial hamming correlation of low-hit-zone frequency hopping sequences and optimal constructions", *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 878-881, Mar. 2018.