Steganography Using Reversible Texture Synthesis

Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE

Abstract—We propose a novel approach for steganography using a reversible texture synthesis. A texture synthesis process resamples a smaller texture image which synthesizes a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography to conceal secret messages. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture. Our approach offers three distinct advantages. First, our scheme offers the embedding capacity that is proportional to the size of the stego texture image. Second, a steganalytic algorithm is not likely to defeat our steganographic approach. Third, the reversible capability inherited from our scheme provides functionality which allows recovery of the source texture. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture.

Index Terms—Data embedding, example-based approach, reversible, steganography, texture synthesis.

I. INTRODUCTION

In the last decade many advances have been made in the area of digital media, and much concern has arisen regarding steganography for digital media. Steganography [1] a singular method of information hiding techniques. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper [2]. A typical steganographic application includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication [3]. In general, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3D model [4], etc. A large number of image steganographic algorithms have been investigated with the increasing popularity and use of digital images [5], [6].

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently, a compromise must be reached between the embedding capacity and the image quality which results in the limited capacity provided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

In this paper, we propose a novel approach for steganography using reversible texture synthesis. A texture synthesis process resamples a small texture image drawn by an artist or captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract the secret messages and the source texture from a stego synthetic texture. To the best of our knowledge, steganography taking advantage of the reversibility has ever been presented within the literature of texture synthesis.

Our approach offers three advantages. First, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional to the size of the stego texture image. Second, a steganalytic algorithm is not likely to defeat this steganographic approach since the stego texture image is composed of a source texture rather than by modifying the existing image contents. Third, the reversible capability inherited from our scheme provides functionality to recover the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce visually plausible texture images, and recover the source texture.
analysis indicates that there is an insignificant probability of breaking down our steganographic approach, and the scheme can resist an RS steganalysis attack [7].

The remainder of this paper is organized as follows: in Section II, we review the texture synthesis techniques. In Section III, we detail our algorithm including embedding and extracting procedures. We describe experimental results and theoretical analysis in Section IV, followed by our conclusions and future work presented in the final section.

II. RELATED WORKS

Texture synthesis has received a lot of attention recently in computer vision and computer graphics [8]. The most recent work has focused on texture synthesis by example, in which a source texture image is re-sampled using either pixel-based or patch-based algorithms to produce a new synthesized texture image with similar local appearance and arbitrary size.

Patch-based algorithms [9], [10], [11] generate the synthesized image pixel by pixel and use spatial neighborhood comparisons to choose the most similar pixel in a sample texture as the output pixel. Since each output pixel is determined by the already synthesized pixels, any wrong synthesized pixels during the process influence the rest of the result causing propagation of errors.

Otori and Kuriyama [12], [13] pioneered the work of combining data coding with pixel-based texture synthesis. Secret messages to be concealed are encoded into colored dotted patterns and they are directly painted on a blank image. A pixel-based algorithm coats the rest of the pixels using the dotted patterns and they are directly painted on a blank image. A secret message to be concealed is encoded into colored dotted patterns and they are directly painted on a blank image. A secret message to be concealed is encoded into colored dotted patterns and they are directly painted on a blank image.

Prokhorov et al. [16] introduced the patch-based sampling strategy and used the feathering approach for the overlapped areas of adjacent patches. Efros and Freeman [17] present a patch stitching approach called “image quilting”. For every new patch that becomes synthesized and stitched, the first algorithm searches the source texture and chooses one candidate patch that satisfies the pre-defined error tolerance with respect to neighbors along the overlapped region. Next, a dynamic programming technique is adopted to disclose the minimum error path through the overlapped region. This declares an optimal boundary between the chosen candidate patch and the synthesized patch, producing visually plausible patch stitching.

Fig. 1. Patch, kernel blocks, and source patch. (a) The diagram of a patch. The central part of a patch is the kernel region; the other part around the kernel region is the boundary region. (b) An illustration of non-overlapped kernel blocks subdivided from the source texture. (c) The diagram of source patches derived by the expanding process using kernel blocks. (d) The boundary mirroring and expanding for a source patch.

Ni et al. [18] proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. Histogram shifting is a preferred technique among existing approaches of reversible image data hiding because it can control the modification to pixels, thus limiting the embedding distortion, and it only requires a small size location map, thereby reducing the overhead encountered. The current state-of-the-art for reversible image data hiding is the general framework presented by Li et al. [19].

To the best of our knowledge, we were unable to disclose any literature that related patch-based texture synthesis with steganography. In this paper, we present our work which takes advantage of the patch-based methods to embed a secret message during the synthesizing procedure. This allows the source texture to be recovered in a message extracting procedure, providing the functionality of reversibility. We detail our method in the next section.

III. PROPOSED METHOD

We illustrate our proposed method in this section. First, we will define some basic terminology to be used in our algorithm. The basic unit used for our steganographic texture synthesis is referred to as a “patch.” A patch represents an image block of a source texture whose size is user-specified. Fig. 1(a) illustrates a diagram of a patch. We can denote the size of a patch by its width (Pw) and height (Ph). A patch contains the central part and an outer part where the central part is referred to as the kernel region with size of Kc×Kc, and the part surrounding the kernel region is referred to as the boundary region with the depth (Pb).

Next, we describe the concept of the kernel block. Given a source texture with the size of Ss×Ss we can subdivide the source texture into a number of non-overlapped kernel blocks, each of which has the size of Kc×Kc, as shown as Fig. 1(b). Let KB represent the collection of all kernel blocks thus generated, and |KB| represent the number of elements in this set. We can employ the indexing for each source patch kb, i.e., KB={kb|i=0 to |KB|-1}. As an example, given a source texture with the size of Ss×Ss=128×128, if we set the size Kc×Kc as 32×32, then we can generate |KB|=16 kernel blocks. Each element in KB
The expanding process will overlap Fig. 1(d) for the kernel block. Our steganographic texture synthesis algorithm needs to operate the boundary mirroring using the kernel block’s symmetric contents to produce the boundary region, as shown in Fig. 1(d) for the kernel block $kb_i$.

Similar to the kernel block, we can denote $SP$ as the collection of all source patches and $SP_n = |SP|$ as the number of elements in the set $SP$. We can employ the indexing for each source patch $sp_i$, i.e., $SP = \{sp_i\}$ where $i = 0$ to $|SP|-1$.

Given a source texture with the size of $S_w \times S_h$, we can derive the number of source patches $SP_n$ using (1) if a kernel block has the size of $K_w \times K_h$. In our paper, we assume the size of the source texture is a factor of the size of the kernel block to ease the complexity.

$$SP_n = \frac{S_w}{K_w} \times \frac{S_h}{K_h}$$

(1)

Our steganographic texture synthesis algorithm needs to generate candidate patches when synthesizing synthetic texture. The concept of a candidate patch is trivial: we employ a window $P_w \times P_h$ and then travel the source texture $(S_w \times S_h)$ by shifting a pixel each time following the scan-line order. Let $CP = \{cp_i\} = \{0, 1, \ldots, CP_n\}$ represent the set of the candidate patches where $CP_n = |CP|$ denotes the number of elements in $CP$. We can derive $CP_n$ using (2).

$$CP_n = |CP| = (S_w - P_w + 1) \times (S_h - P_h + 1)$$

(2)

When generating a candidate patch, we need to ensure that each candidate patch is unique; otherwise, we may extract an incorrect secret message. In our implementation, we employ a flag mechanism. We first check whether the original source texture has any duplicate candidate patches. For a duplicate candidate patch, we set the flag on for the first one. For the rest of the duplicate candidate patches we set the flag off to ensure the uniqueness of the candidate patch in the candidate list.

### A. Message Embedding Procedure

In this section we will illustrate the message embedding procedure. Fig. 2 shows the three processes of our message embedding procedure. We will detail each process in the following sections.

1) **Index Table Generation Process**

The first process is the index table generation where we produce an index table to record the location of the source patch set $SP$ in the synthetic texture. The index table allows us to access the synthetic texture and retrieve the source texture completely. Such a reversible embedding style reveals one of the major benefits our proposed algorithm offers.

We first determine the dimensions of the index table $(T_{pw} \times T_{ph})$. Given the parameters $T_w$, $T_h$, $P_w$, and $P_h$, so that the number of entries is an integer. As an example, if $T_w \times T_h = 488 \times 488$, $P_w \times P_h = 48 \times 48$, and $P_w \times P_h = 8$, then we can generate an index table $(12 \times 12)$ containing 144 entries.

$$TP_n = T_{pw} \times T_{ph} = \left\lfloor \frac{T_{pw}-P_w}{P_w} \right\rfloor + 1 \times \left\lfloor \frac{T_{ph}-P_h}{P_h} \right\rfloor + 1$$

(3)

When we distribute source texture to achieve the manner of reversibility, the source patches can be distributed in a rather sparse manner if the synthetic texture has a resolution that is much larger than that of the source texture, as shown in Fig. 3(a). On the contrary, the source patches may be distributed in a rather dense manner if the synthetic texture has a resolution that is slightly larger than that of the source texture, as shown in Fig. 3(b). For the patch distribution, we avoid positioning a source texture patch on the borders of the synthetic texture. This will encourage the borders to be produced by message-oriented texture synthesis, enhancing the image quality of the synthetic texture. We further define the first-priority position $L_1$ and the second-priority position $L_2$, for two types of priority locations where $||L_1||$ and $||L_2||$, derived in (4), represent the number in the first-priority and second-priority positions, respectively.

$$L_1 = \left\lfloor \frac{T_{pw}-P_w}{P_w} \right\rfloor = \left\lfloor \frac{T_{ph}-P_h}{P_h} \right\rfloor + 1$$

$$L_2 = \left\lfloor \frac{T_{pw}-P_w}{P_w} \right\rfloor + 1 \times \left\lfloor \frac{T_{ph}-P_h}{P_h} \right\rfloor + 1$$

(4)
Given the number of patches $SP_n$ subdivided from the source texture, the strategy of patch distribution is to distribute patches perfectly on the first-priority positions before posting patches on the second-priority positions. Based on the resolution of the synthetic texture, we will have two cases: the sparse distribution and dense distribution. These are described below.

When the number of source patches is less than or equal to the number of the first-priority positions ($SP_n \leq ||L_1||$), the patch will be distributed sparsely. In the security issue section we describe some mathematical analyses of our algorithm. The analysis shows that the total number of patterns that the sparse distribution can offer is $c_{SP_n}^{8 \times 8} \times SP_n!$. On the contrary, when the number of source patches is greater than the first-priority position ($SP_n > ||L_1||$), the patch will be distributed densely. A mathematical analysis shows that the total number of patterns that the dense distribution can offer is $c_{SP_n}^{8 \times 8} \times SP_n!$.

The index table has the initial values of -1 for each entry, which shows that the table is blank. Now, we need to re-assign values when we distribute the source patch ID in the synthetic texture. In our implementation, we employ a random seed for patch ID distribution, which increases the security of our steganographic algorithm making it more difficult for malicious attackers to extract the source texture. As a result, the index table will be scattered with different values as shown in Fig. 4(b) where we have nine source patches (no. 0 to 8) and 135 blank locations with the initial value of “-1”. In this index table, the entries with non-negative values indicate the corresponding source patch ID subdivided in the source texture, while these entries with the value of -1 represent that the patch positions will be synthesized by referring to the secret message in the message-oriented texture synthesis. Taking the above condition into consideration, we can now use the random seed $R$, to disarrange the ID of the source patches subdivided in the source texture. For example, if there are nine source patches ($SP_n=9$) and the synthetic texture is synthesized with a total number of 144 patches ($TP_o=144$), we can distribute the disarranged nine IDs of the source patches resulting in a sparse distribution. Secret messages will be encoded in the remaining 135 blank locations during the message-oriented texture synthesis.

2) Patch Composition Process

The second process of our algorithm is to paste the source patches into a workbench to produce a composition image. First, we establish a blank image as our workbench where the size of the workbench is equal to the synthetic texture. By referring to the source patch IDs stored in the index table, we then paste the source patches into the workbench. During the pasting process, if no overlapping of the source patches is encountered, we paste the source patches directly into the workbench, as shown in Fig. 3(c). However, if pasting locations cause the source patches to overlap each other, we employ the image quilting technique [17] to reduce the visual artifact on the overlapped area.

3) Message-oriented Texture Synthesis Process

We have now generated an index table and a composition image, and have pasted source patches directly into the workbench. We will embed our secret message via the message-oriented texture synthesis to produce the final stego synthetic texture.

The three fundamental differences between our proposed message-oriented texture synthesis and the conventional patch-based texture synthesis are described in Table I. The first difference is the shape of the overlapped area. During the conventional synthesis process, an L-shape overlapped area is normally used to determine the similarity of every candidate patch. In contrast, the shape of the overlapped area in our algorithm varies because we have pasted source patches into the workbench. Consequently, our algorithm needs to provide more flexibility in order to cope with a number of variable shapes formed by the overlapped area.

The second difference lies in the strategy of candidate selection. In conventional texture synthesis, a threshold rank is usually given so that the patch can be randomly selected from candidate patches when their ranks are smaller than the given threshold. In contrast, our algorithm selects “appropriate” patches by taking into consideration secret messages. Finally, the output of the conventional texture synthesis is a pure synthetic texture. However, our algorithm produces a much different synthetic texture. The source texture being converted into a number of source patches has been pasted as part of the contents in the large synthetic texture. In addition, the output large texture has been concealed with the secret message.

While the conventional texture synthesis algorithm has an “L-shape” overlapped area, our algorithm may acquire another four shapes of the overlapped area, as shown in Fig. 5. Assume that the texture synthesis is carried on using the scan-line order. The texture area reveals a typical “L-shape” of an overlapped area, as shown in Fig. 5(a). However, when a nearby pasted source patch has occupied the right side of the working location, this leads to a “downward U-shape” of the overlapped area (Fig. 5(b)). In addition, if a nearby pasted source patch has occupied the bottom side, this leads to a “rightward U-shape” of the overlapped area (Fig. 5(c)). If a nearby pasted source patch has occupied the lower right corner of the working location, this leads to a disjointed overlapped area containing an “L-shape” and a small but isolated part (Fig. 5(d)). Finally, if two nearby

\[
\begin{align*}
||L_1|| &= \frac{T_{pw} T_{ph} - 2}{2} \\
||L_2|| &= \frac{T_{pw} T_{ph} - 2}{2}
\end{align*}
\]
pasted source patches have occupied the right and bottom side of the working location, this will contribute to an “O-shape” of the overlapped area (Fig. 5(e)).

For each candidate patch within the candidate list, one of the five shapes of overlapped area described above will occur when referring to the synthesized area in the working location. Thus, we can compute the mean square error (MSE) of the overlapped region between the synthesized area and the candidate patch. After all MSEs of the patches in the candidate list are determined, we can further rank these candidate patches according to their MSEs. Fig. 6 demonstrates an example of a candidate list where four candidate patches have different MSEs. The candidate patch which has the smallest MSE indicates that this candidate patch is the most similar to the synthesized area in the working location.

Once the ranks of all candidate patches are determined, we can select the candidate patch where its rank equals the decimal value of an n-bit secret message. In this way, a segment of the n-bit secret message has been concealed into the selected patch to be pasted into the working location. In our implementation, we employ a simple but effective image quilting technique [17] to reduce the visual artifact encountered in the overlapped area.

### B. Capacity Determination

The embedding capacity is one concern of the data embedding scheme. Table II summarizes the equations we described to analyze the embedding capacity our algorithm can offer. The embedding capacity our algorithm can offer is related to the capacity in bits that can be concealed at each patch (BPP, bit per patch), and to the number of embeddable patches in the stego synthetic texture (EPn). Each patch can conceal at least one bit of the secret message; thus, the lower bound of BPP will be 1, and the maximal capacity in bits that can be concealed at each patch is the upper bound of BPP, as denoted by $BPP_{max}$. In contrast, if we can select any rank from the candidate list, the upper bound of BPP will be $\left\lceil \log_2(CP_n) \right\rceil$. The total capacity (TC) our algorithm can offer is shown in (5) which is the multiplication of BPP and EPn. The number of the embeddable patches is the difference between the number of patches in the synthetic texture (TPn) and the number of source patches subdivided in the source texture (SPn).

$$TC = BPP \times EP_n = BPP \times (TP_n - SP_n)$$

Suppose we provide a source texture $S_s \times S_h = 128 \times 128$, and we intend to generate a synthetic texture $T_s \times T_h = 488 \times 488$. We specify the patch size $P_w \times P_h = 48 \times 48$ and the boundary depth $P_d$.

### C. Source Texture Recovery, Message Extraction, and Message Authentication Procedure

The message extracting for the receiver side involves generating the index table, retrieving the source texture, performing the texture synthesis, and extracting and authenticating the secret message concealed in the stego synthetic texture. The extracting procedure contains four steps, as shown in Fig. 7.

Given the secret key held in the receiver side, the same index table as the embedding procedure can be generated. The next step is the source texture recovery. Each kernel region with the size of $K_s \times K_h$ and its corresponding order with respect to the size of $S_s \times S_h$ source texture can be retrieved by referring to the index table with the dimensions $T_{mu} \times T_{ph}$. We can then arrange kernel blocks based on their order, thus retrieving the recovered source texture which will be exactly the same as the source texture. In the third step, we apply the composition image generation to paste the source patches into a workbench to produce a composition image by referring to the index table. This generates a composition image that is identical to the one produced in the embedding procedure.

The final step is the message extraction and authentication step, which contains three sub-steps. The first sub-step constructs a candidate list based on the overlapped area by referring to the current working location. This sub-step is the
same as the embedding procedure, producing the same number of candidate lists and their corresponding ranks.

The second sub-step is the match-authentication step. Given the current working location Cur(WL) on the workbench, we refer to the corresponding stego synthetic texture at the same working location Stg(WL) to determine the stego kernel region Sk×Sk then, based on this stego kernel region, we search the candidate list to determine if there is a patch in the candidate list where its kernel region is the same as this stego kernel region. If this patch is available, we refer to it as the matched patch, and denote it as MKp×MKp. Clearly, we can locate the rank R of the matched patch, and this rank represents the decimal value of the secret bits we conveyed in the stego patch when operating the texture synthesis in the message embedding procedure. However, if we cannot disclose any matched patch in the candidate list where the kernel region is the same as the stego kernel region, it means that the stego kernel region has been tampered with, leading to a failure of the message authentication. In this way, we can authenticate and extract all of the secret messages that are concealed in the stego synthetic texture patch by patch.

Our method is resistant against malicious attacks as long as the contents of the stego image are not changed. With some side information, for example, our scheme can survive the attacks of the image mirroring or image rotation by 90, 180, or 270 degrees. Nevertheless, if malicious attacks lead to alteration of the contents of the stego texture image, the message authentication step will justify the authenticity of the secret messages.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Results of the Embedding Capacity

We collect our experimental results on a personal computer with an i7-2600 3.4GHz CPU and 4GB memory. We adopt four source textures for the results of our collection. Table III presents the total embedding capacity our algorithm can provide when different resolutions of the synthetic texture are produced by concealing various BPPs. It is interesting to point out that given a fixed number of BPP, the larger the resolutions of the source texture S×S (96×96 vs. 192×192), the smaller the total embedding capacity (TC) our algorithm will offer (6160 bits vs. 5890 bits for 10 BPP). This is because the larger source texture will contain more source patches SP in (9 vs. 36) that we need to paste which cannot conceal any secret bits. This will reduce the number of embeddable patches (EP) on the composition image (616 vs. 589), thus reducing the total embedding capacity. Nevertheless, we can employ larger BPP (11 vs. 14) in order to convey more secret messages (6776 bits vs. 8246 bits). The maximal capacity provided by our algorithm is 34398 bits.

We compare our embedding capacity with the work presented by Otori and Kuriyama [13]. In their algorithm, a data-coded texture image of 480×640 pixels contains 5×5 or 10×10 dotted patterns, thus concealing the capacity in the range of 200 to 800 bits. In contrast, our scheme conveys the capacity ranging from 12285 to 34398 bits in a stego texture synthesis image of 1024×1024 pixels. Consequently, the capacity we offer varies from 4.50 to 50.39 times more than our counterparts. Besides, our scheme extracts the secret messages correctly, while their scheme exhibits a small error rate when extracting secret messages.

Fig. 8 compares stego synthetic textures with different capacities. We also present the pure synthetic texture which does not convey any secret message. No significant visual difference exists between the two stego synthetic textures and the pure synthetic texture. In addition, no significant visual difference can be perceived when comparing two stego synthetic textures embedded by 5 BPP vs. 10 BPP.

The computing times of Fig. 6 are shown in Table IV. The range of the computing time is 6.8% to 8.7% more than that needed for pure texture synthesis. Nevertheless, our algorithm is flexible enough to provide a different embedding capacity by simply altering the patch size, satisfying the desirable capacity or texture quality demanded by users. Also, our algorithm can retrieve the source texture, making possible the second round of message embedding using the recovered source texture.

B. Image Quality Comparison

We use several mechanisms to determine the image quality of the stego synthetic texture. We define the first measurement, which is called the mean squared error of the overlapped area (MSEO) to determine the image quality of the synthetic results. MSEO reflects the similarity between the candidate patch and the synthesized area where we will specifically operate the

![Flowchart of the four-step message extracting procedure](image_url)
image quilting technique during the message-oriented texture synthesis process. Consequently, the MSEO has a non-zero value even in the case of the pure patch-based texture synthesis. If the MSEO produces a small value, it implies that the synthetic texture shows a high image quality of the overlapped areas. Obviously, the lower the MSEO value, the higher quality of the synthetic texture image. The equation of MSEO is shown in (6), where OL_{i} stands for the overlapped area of the working location, \( p_{ij} \) stands for the pixel \( j \) of the candidate patch in OL_{i}, and \( p_{ij}^{\prime} \) stands for the pixel \( j \) of the synthesized area in OL_{i}.

\[
\text{MSEO} = \frac{1}{(EP_{h})_{x}P_{w}P_{d}} \sum_{i=1}^{EP_{h}} \sum_{j \in OL_{i}} \left( p_{ij}^{\prime} - p_{ij} \right)^{2}
\]

The MSEO can be calculated during the texture synthesis procedure. When we synthesize a patch, we accumulate the squared errors of all the pixels in the overlapped area between the synthesized area and the selected candidate patch. When the texture synthesis procedure is finished, we can divide the summation of squared errors by the patch size and the number of the synthesized patches to produce the MSEO. It comes as no surprise that the MSEO is dependent on the capacity per patch.

Table V compares the MSEO to the embedding capacity for the four test source textures. When we consider the same patch size, the MSEO increases as we convey more secret bits per patch. These MSEO values coincide with the image quality when visualizing the stego synthetic texture. For a larger patch size, the boundary depth increases leading to a larger MSEO. Taking the test source texture “peanuts” as an example, the MSEO is 1034.6 when conveying 5 bits of secret message per patch, while it shows the MSEO of 1236.9 when conveying 10 bits per patch. Fig. 8(c) shows a slightly higher visual image quality than Fig. 8(d).

The second scheme we adopt for measuring the image quality is the Pearson Product Moment Correlation (PPMC) [20]. It is employed as a measure of how well two variables are related. The Pearson coefficient values that this scheme produces are between 1 and -1. A result of 1 means that there is a perfect positive correlation between the two variables, while a result between 0.5 and 1.0 represents a high correlation.

Table VI shows average Pearson coefficients across three R-G-B channels measured under the base of the histogram produced for each channel. In Case-A and Case-B, we reveal the Pearson coefficients between the stego synthetic textures and the pure synthetic texture. We report in Case-C the Pearson coefficients between two stego synthetic textures with different BPPs. The Pearson coefficients shown in Case-A are very close to 1.0. This represents the high correlation between the pure and stego synthetic textures. In Case-B, although the Pearson coefficient values slightly decrease along with the increase of the embedding capacity per patch, they retain the feature of a close relation between the pure and stego synthetic textures. The Pearson coefficients in Case-C are very close as well, which indicates that the stego synthetic textures conveying 5 BPP remain highly correlated to those conveying 10 BPP. All the Pearson coefficients shown in this table exhibit that our steganographic algorithm is effective in producing stego synthetic textures of high image quality in comparison to pure synthetic textures produced by conventional texture synthesis.

Next, we employ the SSIM (Structural SIMilarity) index [21] to quantify the similarity between the pure and stego synthetic textures. The SSIM is an image quality assessment method for
measuring the change in luminance, contrast, and structure in an image. The SSIM index is in the range of [-1, 1] and when it equals to 1, the two images are identical. Table VII shows the SSIM indices for different patch sizes.

```
| Patch size: \( P_w \times P_h = 48 \times 48 \), boundary depth: \( P_d = 8 \) |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Pure vs. \( P_w \times P_h = 5 \) BPP | Pure vs. \( P_w \times P_h = 10 \) BPP | Pure vs. \( P_w \times P_h = 5 \) BPP vs. \( P_w \times P_h = 10 \) BPP |
| Rope net        | 0.9991          | 0.9991          | 0.9987          |
| Metal           | 0.9990          | 0.9984          | 0.9995          |
| Peanuts         | 0.9980          | 0.9974          | 0.9993          |
| Ganache         | 0.9991          | 0.9955          | 0.9980          |
```

Table VIII shows the SSIM index values for different message probabilities. The SSIM index is highly sensitive to translation and scaling. This explains the low index values shown in Table VII because the patch-based method generates an entirely new synthetic texture image from a number of patches in the source texture resulting in a different level of image translation and scaling.

### C. Results of Different Message Probabilities

The secret messages consist of bit stream “0” or “1.” The experimental results shown so far consider that bit “0” or “1” has equal probability of appearance. However, equal probability may not be the case for some kinds of information to be served as a secret message. We generalize our scheme by considering the probability of appearance.

Let \( p \) represent the probability of appearance of secret bit “1.” If we consider two bits of the secret message, then the probability for bit patterns “00” is \((1-p)(1-p)\). Let \( ER(p,2) \) represent the expected rank of the selected candidate during our message-oriented texture synthesis with \( BPP=2 \). Then, \( ER(p,2) \) can be derived as a function of probability \( p \), as shown in (7).

\[
ER(p, 2) = 0 \times (1 - p)(1 - p) + 1 \times (1 - p)p + 2 \times p(1 - p) + 3 \times p^2 = 3p
\]

In general, when we consider \( BPP=k \) bits of the secret message, we can expect the expected rank of a selected candidate as a more general form, as \( ER(p, k) \) shown in (8). For example, if \( k=10 \) and \( p=0.5 \), \( ER(0.5,10)\approx511.5 \). However, if \( p=0.7 \), then \( ER(0.7,10)\approx716.1 \). If we select the larger rank, the larger MSEO would be expected. Consequently, the image quality of the synthetic texture is likely to be worse than the one produced by \( p=0.5 \). In general, if \( p \) is smaller, we are likely to select a better candidate of patch, which leads to producing a better stego synthetic texture. Thus, our algorithm is general enough to cope with the situation when given a variety of \( p \) values.

Table VIII shows the MSEO with the different probability \( p \). The statistics show that this larger probability causes the increase of MSEO, as expected. This is due to the fact that when the secret message has the larger probability \( p \), the candidate patch is likely to be selected at the rear part of the candidate list, leading to larger MSEO.

To improve the probability of getting better ranks we can conduct the “probability complement” process to decrease the MSEO. If the probability \( p \) is larger than 0.5, we adopt the probability of \( 1-p \) for message embedding. This can be realized by flipping every bit of the secret message to its reverse style. During the extraction stage, we extract the secret bit as usual, and then flip it again to produce the correct message. With this mechanism, we can ensure that the probability used for message embedding is always less than or equal to 0.5, which encourages our scheme to produce a stego synthetic texture with a smaller MSEO. Clearly, we need to adopt a secret key to record whether or not we have conducted any flipping operation.

If we are not able to determine the probability of the secret message, such as the example of the message being from a streaming source, then we can use a strategy referred to as “probability balancing” to produce a nearly even probability of \( p=0.5 \). In particular, we can conduct an XOR operation between the previous message clip \( M_{i-1} \) and the current message clip \( M_i \). For example, if we want to embed \( M_i \) to patch \( i \), we do the XOR
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI

The eavesdropper may try to speculate about the contents of the index table. For the case of the sparse distribution, the number of patterns from 2-bit to 12-bit is \( P_{bc} = 0.1 \). The overall probability that an eavesdropper can retrieve source texture will be \( P_{b} = P_{b}^{sp} \times P_{b}^{de} = 1.18 \times 10^{-22} \).

For the dense distribution we employ a larger source texture \( S_{m} = 192 \times 192 \). An eavesdropper can retrieve \( SP_{n} = 36 \), \( T_{m} \times T_{m} = 12 \times 12 \), and \( ||L_{1}|| = 25 \). The probability that an index table has broken down is \( P_{b} = 8.70 \times 10^{-49} \). The overall probability that an eavesdropper can retrieve source texture will be \( P_{b} = P_{b}^{sp} \times P_{b}^{de} = 4.35 \times 10^{-51} \). Both examples illustrate that even though the security of level one has collapsed, there is insignificant probability that our steganographic system can be attacked to retrieve the source texture, and consequently, the secret message. The analysis indicates that our steganographic system is secure against a malicious attack.

### Table IX

<table>
<thead>
<tr>
<th>Channels</th>
<th>Capacity</th>
<th>( Rm+ )</th>
<th>( Rm- )</th>
<th>( Sm+ )</th>
<th>( Sm- )</th>
</tr>
</thead>
<tbody>
<tr>
<td>R channel</td>
<td>5 BPP</td>
<td>30.48</td>
<td>35.77</td>
<td>21.66</td>
<td>16.99</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>29.72</td>
<td>35.77</td>
<td>21.45</td>
<td>16.82</td>
</tr>
<tr>
<td>G channel</td>
<td>5 BPP</td>
<td>30.70</td>
<td>32.28</td>
<td>20.49</td>
<td>19.71</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>30.94</td>
<td>32.26</td>
<td>20.51</td>
<td>19.97</td>
</tr>
<tr>
<td>B channel</td>
<td>5 BPP</td>
<td>31.99</td>
<td>31.55</td>
<td>19.44</td>
<td>20.19</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>32.32</td>
<td>31.87</td>
<td>19.86</td>
<td>20.43</td>
</tr>
</tbody>
</table>

### Table X

<table>
<thead>
<tr>
<th>Channels</th>
<th>Capacity</th>
<th>( Rm+ )</th>
<th>( Rm- )</th>
<th>( Sm+ )</th>
<th>( Sm- )</th>
</tr>
</thead>
<tbody>
<tr>
<td>R channel</td>
<td>5 BPP</td>
<td>30.48</td>
<td>35.77</td>
<td>21.66</td>
<td>16.99</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>29.72</td>
<td>35.77</td>
<td>21.45</td>
<td>16.82</td>
</tr>
<tr>
<td>G channel</td>
<td>5 BPP</td>
<td>30.70</td>
<td>32.28</td>
<td>20.49</td>
<td>19.71</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>30.94</td>
<td>32.26</td>
<td>20.51</td>
<td>19.97</td>
</tr>
<tr>
<td>B channel</td>
<td>5 BPP</td>
<td>31.99</td>
<td>31.55</td>
<td>19.44</td>
<td>20.19</td>
</tr>
<tr>
<td></td>
<td>10 BPP</td>
<td>32.32</td>
<td>31.87</td>
<td>19.86</td>
<td>20.43</td>
</tr>
</tbody>
</table>

operation and produce \( M' _i = M_i \oplus M'_{i-1} \). Then, we embed \( M' _i \) to patch \( i \). In the extraction procedure, we recover the secret clip \( M_i \) with another XOR operation, where \( M_i = M' _i \oplus M'_{i-1} \). With this mechanism, we can produce a stego synthetic texture where its image quality is close to the one produced by \( p=0.5 \), free from the effect of message probability.

Table IX shows the effect of “probability balancing.” The results show that all of the MSEOs are close to those produced with the probability \( p=0.5 \) regardless of using different message probabilities.

### D. Security Issue

In this section we discuss the probability of breaking our steganographic algorithm in order to produce a correct secret message. We assume the resolution of the stego synthetic texture is known by the eavesdropper.

We explain our first level of security. For four possible squared sizes of the source texture \( (S_{m} \times S_{m}) \), the probability of breaking down is \( P_{b} = 0.25 \). The probability of breaking down five possible squared sizes of the patch \( (P_{n} \times P_{n}) \) is \( P_{b} = 0.2 \). Finally, the probability of breaking down ten possible BPPs from 2-bit to 12-bit is \( P_{b} = 0.1 \). The total probability that the eavesdropper can break down the security of level one is \( P_{b} = P_{b}^{sp} \times P_{b}^{de} = 1.18 \times 10^{-22} \).

Next, we discuss the second level of security. An eavesdropper might be able to perceive the index table. If the length of the seed used to generate the index table is a 128-bit sequence, it is highly impossible that this seed will be revealed. The eavesdropper may try to speculate about the contents of the index table. For the case of the sparse distribution, the number of source patches \( (SP_{n}) \) is less than or equal to the number of the first-priority position \( (||L_{1}||) \). Thus, the total number of patterns offered is \( C_{SP_{n}}^{||L_{1}||} \times SP_{n}^{4} \). The probability of revealing the correct order of patches in the index table is shown in (9).

For the case of the dense distribution, the number of source patches is larger than the number of the first-priority position \( (SP_{n} > ||L_{1}||) \). Therefore, the total number of permutation patterns that the dense distribution can offer is \( C_{SP_{n}}^{||L_{1}||} \times SP_{n}^{4} \). Thus, the probability of revealing the correct order of these IDs in the index table is shown in (10).

We present two examples to provide more insight for the sparse distribution. Suppose \( T_{m} \times T_{m} = 488 \times 488 \), \( P_{m} \times P_{m} = 48 \times 48 \), \( P_{n} = 8 \), and \( S_{m} \times S_{m} = 128 \times 128 \), where the notations of these variables can be referred to Table II. The eavesdropper can retrieve the number of source patches as \( SP_{n} = 16 \), the dimensions of the index table as \( T_{m} \times T_{m} = 12 \times 12 \), the number of first-priority positions \( ||L_{1}|| = 25 \), and the number of second-priority positions \( ||L_{2}|| = 25 \). An eavesdropper can realize that the case of the sparse distribution is being employed. The probability that the index table is broken down is \( P_{b} = 2.35 \times 10^{-20} \). Even though the security of level one has collapsed, the probability that an eavesdropper can retrieve source texture will be \( P_{b} = P_{b}^{sp} \times P_{b}^{de} = 1.18 \times 10^{-22} \).

### E. Steganalysis

We have determined so far that our scheme is secure. However, we need to conduct steganalysis, the art and science of detecting hidden messages using steganography. While there are a number of steganalysis algorithms developed, we employ the RS steganalytic scheme [7] since this algorithm is well-known, having been adopted for most steganalysis attacks.

In the RS detection method, the relative number of regular groups for masks \( M=[0 \ 1 \ 1 \ 0] \) and \( -M=[0 \ -1 \ -1 \ 0] \) is denoted as \( (R_{m}, R_{m}) \). Similarly, the relative number of singular groups for masks \( M \) and \( -M \) is denoted as \( (S_{m}, S_{m}) \). If the magnitude of \( R_{m} \) is equal to that of \( R_{m} \), the same equivalence happens to the singular group \( (S_{m}, S_{m}) \). The embedded image will pass the RS steganalysis. Otherwise, it would reveal the presence of the secret message.

In detection processing, we compute the absolute difference of the regular group \( |R_{m} - R_{m}| \) and that of the singular group \( |S_{m} - S_{m}| \) with masks \( M=[0 \ 1 \ 1 \ 0] \) and \( -M=[0 \ -1 \ -1 \ 0] \). A small difference usually means that the stego image is more secure to the RS steganalysis.

Table X shows the detection results for the source texture “rope net” in three primary color channels. Even though each patch is concealed with different amounts of secret bits, the difference between regular group \( R_{m} \) and \( R_{m} \) is similar to the values shown for the pure synthetic texture. This similar difference invariance reflects for singular groups \( S_{m} \) and \( S_{m} \). These statistics indicate our message-oriented texture synthesis.
algorithm can resist the RS detection attack. This is due to the fact that the secret bits are concealed by selecting different ranks of candidate patches rather than by modifying their contents.

V. CONCLUSIONS AND FUTURE WORK

This paper proposes a reversible steganographic algorithm using texture synthesis. Given an original source texture, our scheme can produce a large stego synthetic texture concealing secret messages. To the best of our knowledge, we are the first that can exquisitely weave the steganography into a conventional patch-based texture synthesis. Our method is novel and provides reversibility to retrieve the original source texture from the stego synthetic textures, making possible a second round of texture synthesis if needed. With the two techniques we have introduced, our algorithm can produce visually plausible stego synthetic textures even if the secret messages consisting of bit “0” or “1” have an uneven appearance of probabilities. The presented algorithm is secure and robust against an RS steganalysis attack. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications.

One possible future study is to expand our scheme to support other kinds of texture synthesis approaches to improve the image quality of the synthetic textures. Another possible study would be to combine other steganography approaches to increase the embedding capacities.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. We would like to express our special thanks of gratitude to Dr. Evelyne Pickett for her enthusiastic assistance in improving the clarity of this article.

REFERENCES


Kuo-Chen Wu is a Ph.D. student in the Department of Computer Science and Engineering at National Chung Hsing University, Taiwan. He received the M.Sc. degree from the Department of Computer Science and Engineering, National Chung Hsing University, Taiwan in 2006. His current research interests include computer graphics, color science, image processing, watermarking, and steganography.

Chung-Ming Wang (M’96) received the B.S. degree in Applied Mathematics from the National Chung Hsing University, Taiwan, in 1984, and the Ph.D. degree in Computer Science from the University of Leeds, Leeds, U.K., in 1992. From August 1986 to August 1988, he was a system analyst in the President Enterprise Cooperation and the PAL Company. He is currently a professor in the Department of Computer Science and Engineering, National Chung Hsing University, Taiwan. His research interests include computer graphics, color science, virtual reality, multimedia systems, watermarking, and steganography. Dr. Wang has won three Dragon Thesis Awards, funded by the Acer Computers, and the two Outstanding Paper Awards from the Computer Society of the Republic of China. He is a member of ACM and IEEE Computer Society.