2005－ＣＳＥＣ－30 (58)
2005／7／22

予測符号化を用いた可逆電子透かし

栗林 稔† 森井 昌克† 田中 初一††

† 神戸大学工学部 〒657-8501 神戸市灘区六甲台町 1-1
†† 神戸情報大学院大学 〒650-0001 神戸市中央区加納町 2-2-7
E-mail: †{kminoru,mmorii}@kobe-u.ac.jp, ††tanaka@kic.ac.jp

あらまし 透かし情報の埋め込まれた画像から，透かし情報だけでなく元の画像を完全に復元できる電子透かし技術は可逆電子透かしと呼ばれている．最初に LSB に透かし情報を埋め込む手法が提案され，その後整数変換やウェーブレット変換などを用いた手法が提案された．本論文では，画質劣化を抑えて埋め込める情報量を増加させるために JPEG-LS で採用されている予測符号化の技術を使って求めた予測誤差に透かし情報を埋め込む手法を提案する．予測値は前出の画素値に依存しており，わずかな誤差に対しても非常に敏感に変化する．この特性に基づいて，埋め込みの際に用いる秘密鍵が分からなければ透かし情報を取り出すことが困難となる可逆電子透かし方式を提案する．

キーワード 可逆電子透かし，予測符号化，JPEG-LS

A Secure Reversible Watermark Using Predictive Coding

Minoru KURIBAYASHI†, Masakatu MORII†, and Hatsukazu TANAKA††

† Faculty of Engineering, Kobe University, 1-1, Rokkodai, Nada, Kobe, 657-8501
†† Kobe Institute of Computing, Kanou-cho 2-2-7, Chuo-ku, Kobe, 650-0001
E-mail: †{kminoru,mmorii}@kobe-u.ac.jp, ††tanaka@kic.ac.jp

Abstract The watermark that restores the exact original image from the watermarked one is called reversible watermark. Firstly, the LSB data embedding method had been proposed and the variants using integer transform and wavelet transform were proposed. In this paper, a watermark is embedded into prediction errors calculated using a predictive coding technique in JPEG-LS to increase the information to be embedded with less degradation. Since the predictor is strongly dependent on the previous pixel values, a tiny change in one pixel value propagates to the following prediction values. Based on the property, we propose a secure reversible watermarking scheme such that a watermark cannot be recovered without a secret key used at the embedding operation.

Key words reversible watermark, predictive coding, JPEG-LS

1. Introduction

In data-hiding technique, an information is inserted into multimedia contents without introducing perceptual artifacts [1]. The technique has a potential for a lot of applications such as copyright protection, authentication of the integrity, tracing illegal users, etc.. In general, the embedding causes irreversible degradation to an image. Although the degradation is perceptually slight, it may not be accepted to some applications such as medical or military images. Reversible watermark technique can completely remove the distortions and recover the original image in the extraction process.

The reversible watermark technique may be classified into two methods. One compresses features of an image and transmits the compressed bit stream as a part of the embedding information. At the decoding, the embedded information including the compressed bit stream is extracted, and the original image is restored by replacing the modified features with the decompressed original features. In [2], each pixel is first quantized by a quantization step size L, and appends the embedding information to the compressed quantization noise. Then, the information is added to the quantized image. The other method uses reversible integer transforms to the spatial domain of an image, and embeds a watermark information in the transformed signal values. It requires a control of the embedding operation to avoid overflow and underflow of the values because of the limited *range in* the pixel value. So as to recover the original image, an additional information for the control which is called a location map is required. Therefore, the map is embedded as a part of the embedding information after compression. Tian [3] presented a difference expansion transform of a pair of pixels, which is haar wavelet transform, to devise a high capacity and low degradation reversible watermark. Alattar [4] extends the difference expansion of a vectors instead of pairs to achieve a high capacity. The algorithm hides several bits in the difference expansion of each vector of adjacent pixels. In the above conventional scheme, however, the secrecy of the embedded watermark is not considered. Because one can extract the watermark without any information like a secret key, the modification of the watermark information may be possible.

In this paper, we propose a new technique to embed an information in prediction errors calculated by well-designed predictor in JPEG-LS [5]. Since the average value of the prediction errors is small, our scheme can increase the positions where a watermark can be embedded without both overflow and underflow. Such property contributes to increase the capacity of the reversible watermark. We also focus on the dependency of the prediction value with the previous pixel values, which is exploited to enhance the secrecy from unauthorized party. Without the accurate prediction based on a secret key, both the extraction of the watermark ans recovery of the original image are difficult.

2. Modeling in JPEG-LS

JPEG-LS [5] is the algorithm at the core of the new IS/ITU standard for lossless and near-lossless compression. The algorithm attains significantly better compression ratios, similar or superior to those obtained with state-of-the art schemes based on arithmetic coding, but at a fraction of the complexity.

Lossless image compression schemes, in general, consist of two distinct and independent components:*modeling* and *coding*. The modeling part is formulated as an inductive inference problem, in which an image is observed sample by sample in some predefined order. In JPEG-LS, the sample points are defined as a, b, c, and d in Fig.1. And the current

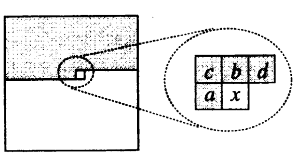

Fig. 1 The fixed predictors a, b, c, and d

sample x is predicted as $\hat{x}$ using the four samples. In the coding part, the predictive error ϵ

$$\epsilon = x - \hat{x} \tag{1}$$

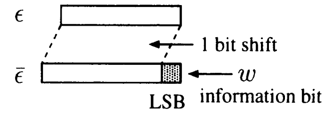

Fig. 2 Expanding of the prediction error to embed a watermark.

is encoded with an extended family of Golomb-type code [7] which is adaptive symbol-by-symbol coding at very low complexity.

The distribution of the prediction error ϵ is well modeled by a *two-sided geometric distribution* (TSGD) [6] centered at zero. And ϵ is also extremely sensitive for the changes in the previously occurred samples. The change occurred in one sample is propagating to the following every prediction error, and the distribution is almost random. Applying such properties, we propose an algorithm for reversible watermark with high secrecy.

3. Proposed Reversible Watermark

In this section, we propose a new reversible watermark scheme using the predictive coding technique in JPEG-LS. First, a basic algorithm of the reversible operation for the embedding is shown. In the algorithm, the secrecy of the embedded watermark is not considered. Then, the algorithm is modified by introducing a randomization of the prediction error using a secret information.

3.1 Preliminary

The main idea of our scheme is to utilize the prediction errors calculated by the predictor and the modeling in JPEG-LS to embed information bits in an image. Since the prediction errors follow TSGD centered at zero, the average value might be small.

The basic embedding operation is to double ϵ, and to put an information bit w on its LSB(See Fig.2).

$$\bar{\epsilon} = 2\epsilon, \tag{2}$$

It seems difficult to modify the prediction error using the previously occurred pixels a, b, c, and d because those pixels are also used for the prediction of other pixels. Instead, we modify the current target pixel x, which is easily calculated from Eq.(1).

$$x' = x + \epsilon + w \tag{3}$$

Here, it must be considered that the pixel value must be in $[0, 255]$, otherwise it causes overflow(more than 255) or underflow(less than 0). So as to control the embedding operation, the following definition is introduced.

[Definition 1] The pixel x is said to be expandable if, for any $w \in \{0, 1\}$, x can be modified to x' without causing overflow and underflow.

If a pixel is expandable, it is possible to embed an information bit in the LSB by expanding the prediction error ϵ.

However, when one wants to extract an information, it is impossible to find if the pixel was expandable or not before the embedding. By considering the extraction, the prediction errors of the pixels which are not expandable are modified to even number by the following equation.

$$x^{\star} = \begin{cases} x-1 & if\ \epsilon\ is\ odd \\ x & otherwise. \end{cases} \quad (4)$$

Then the LSB of the prediction error is removed. So as to be reversible, the LSB of those pixels are embedded with a watermark information. Here, the overflow and underflow of $x^{\star}$ must be considered. Therefore, the following definition is also introduced.

[**Definition** 2] The pixel x is said to be changeable if, for any $w \in \{0,1\}$, x can be modified to x'' without causing overflow and underflow.

$$x'' = x^{\star} + w \quad (5)$$

Notice that all expandable pixels are changeable and they are still changeable after the embedding. Based on the characteristic, for both expandable and changeable pixels, information bits are embedded into the LSBs of their prediction errors, which are extracted from all changeable pixels of the watermarked image. Although the watermark can be extracted, it is impossible to determine if each pixel was expandable or changeable before embedding. Hence, the information about the original conditions of pixels which is called location map is embedded additionally with a watermark. Although the size of the map is large, a lossless compression algorithm, such as JBIG and an arithmetic compression algorithm, may be applicable. As the consequence, the embedding information bits are composed by three parts, a compressed location map, LSB of ϵ of changeable pixel, and a watermark information.

3.2 Basic Algorithm

Each pixel can be classified into three groups according to the Definition 1 and 2. The first group S_1 contains all expandable pixels whose prediction errors less than a predefined threshold T. The second group S_2 contains all changeable pixels that are not in S_1. The third group S_3 contains the rest of the pixels which implies not changeable. Also, let S_4 denote all changeable pixels ($S_4 = S1 \cap S_2$).

In general, there is a trade-off between the distortions and the capacity in watermarking technique, and it is desirable that the trade-off is controlled for applications. In our scheme, it is achieved by introducing a threshold T for the determination of expandable or not. If the absolute value of a prediction error is less than T and Definition 1 is satisfied, the pixel is regarded expandable. Since the changes caused by the operation in expandable pixels are restricted less than T, the degradation of the quality is controlled.

The proposed algorithm is composed by four parts: *formatting*, *embedding*, *extraction*, and *recovery*. The summaries of the operations are shown below.

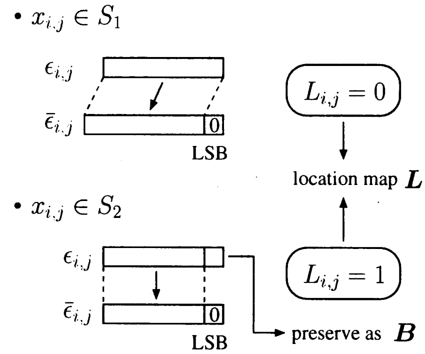

Fig. 3 Formatting operation.

Formatting: For a scanned pixel $x_{i,j}, (0 \leq i \leq N-1, 0 \leq j \leq M-1)$ by a raster scan order, the following operations are performed.

(1) Calculate the prediction error $\epsilon_{i,j}$ using Eq.(1).

(2) Modify $x_{i,j}$ to $\bar{x}_{i,j}$ based on the following three conditions.

$$\bar{x}_{i,j} = \begin{cases} x_{i,j} + \epsilon_{i,j} & if\ x_{i,j} \in S_1 \\ x_{i,j} - 1 & if\ x_{i,j} \in S_2\ and\ \epsilon_{i,j}\ is\ odd \\ x_{i,j} & otherwise \end{cases} \quad (6)$$

The modification implies,

$$\bar{\epsilon}_{i,j} = \begin{cases} 2\epsilon_{i,j} & if\ x_{i,j} \in S_1 \\ \epsilon_{i,j} - 1 & if\ x_{i,j} \in S_2\ and\ \epsilon_{i,j}\ is\ odd \\ \epsilon_{i,j} & otherwise \end{cases} \quad (7)$$

After the above modification, the prediction error $\bar{\epsilon}_{i,j}$ becomes even number if $x_{i,j} \in S_4$.

(3) If $x_{i,j} \in S_1$, then the location map is set to $L_{i,j} = 0$, else $L_{i,j} = 1$.

(4) If $x_{i,j} \in S_2$, the LSB of $\epsilon_{i,j}$ is added to a vector $\boldsymbol{B}$ as one element.

Figure 3 illustrates the formatting operation.

[**Remark** 1] For the prediction of a current pixel $x_{i,j}$, the previously formatted four pixels which are specified in Fig.1 are used.

The location map $L_{i,j}$ is compressed by JBIG. We call the bit-stream of the compressed map $\boldsymbol{L}$. Then $\boldsymbol{L}$, $\boldsymbol{B}$, and a watermark information bit-stream $\boldsymbol{W}$ is embedded. Combining those bit-streams, the embedding information $\boldsymbol{w}$ is produced.

$$\boldsymbol{w} = \{\boldsymbol{head}||\boldsymbol{L}||\boldsymbol{B}||\boldsymbol{W}\} \quad (8)$$
$$= \{w_1, w_2, \ldots, w_{\sigma}\} \quad (9)$$

Where ***head*** is a header file of the embedding information, $||$ means concatenation, and σ is the bit-length of W.

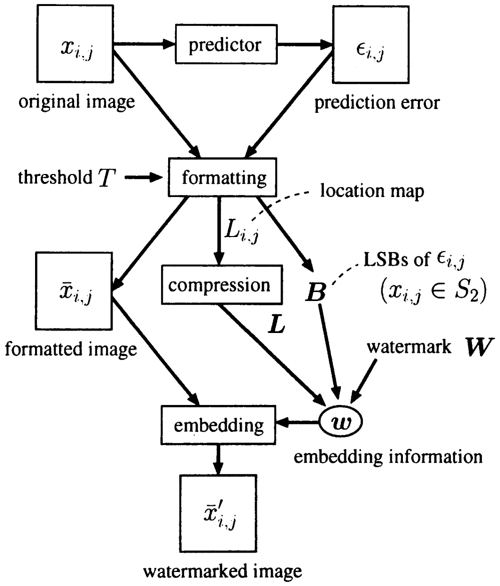

Fig. 4 The flow of the algorithm (*formatting* and *embedding*).

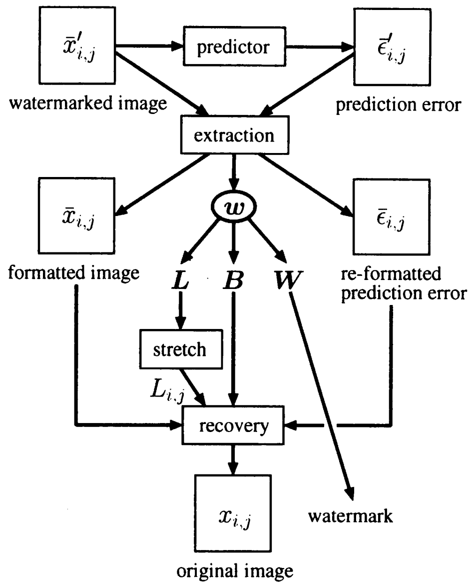

Fig. 5 The flow of the algorithm (*extraction* and *recovery*).

Embedding: After the above formatting, every prediction error, not pixel value, becomes even number. The embedding operation is simply to add each information bit of w directly to each pixel $x_{i,j} \in S_4$ by raster scan order.

By setting a counter $t = 1$, the following operations are performed repeatedly for each formatted pixel $\bar{x}_{i,j}$.

(1) Modify $\bar{x}_{i,j}$ to $\bar{x}'_{i,j}$ using the embedding information bit w_t

$$\bar{x}'_{i,j} = \begin{cases} \bar{x}_{i,j} + w_t & if\ x_{i,j} \in S_4 \\ \bar{x}_{i,j} & otherwise \end{cases} \tag{10}$$

(2) If $t < \sigma$, increment $t = t + 1$ and go back to (1), otherwise finished.

By the *formatting* and *embedding*, watermarked image is obtained. The flow of the algorithm is depicted in Fig.4

Extraction: When the embedded information is extracted, each information bit is extracted from each pixel by a raster scan order. Since each prediction error is calculated from the previously formatted four pixels, the same pixels are required for the prediction at the extraction. Therefore, the extraction is performed by the following steps for each raster scanned pixel.

(1) Set a counter $t = 1$.

(2) Calculate the prediction error $\epsilon_{i,j}$ for a target pixel $\bar{x}'_{i,j}$.

(3) If $\bar{x}'_{i,j}$ is changeable, which implies $\bar{x}'_{i,j} \in S4$, then the following operations are performed.

(3-1) Extract the LSB of $\bar{\epsilon}'_{i,j}$ as t-th embedding information bit w_t.

$$w_t = \bar{\epsilon}'_{i,j} \pmod 2, \tag{11}$$

(3-2) In order to make the prediction error even number, subtract w_t from $\bar{x}'_{i,j}$.

$$\bar{x}_{i,j} = \bar{x}'_{i,j} - w_t \tag{12}$$

(3-3) Store the re-formatted prediction error $\bar{\epsilon}_{i,j}$.

$$\bar{\epsilon}_{i,j} = \bar{\epsilon}'_{i,j} - w_t \tag{13}$$

(3-4) Increment $t = t + 1$.

(4) Perform the above operation (2) and (3) using the re-formatted four pixels until all pixels are checked.

Recovery: After the *extraction*, w is completely extracted and the original formatted image is recovered. Then the original image is recovered using w and each re-formatted prediction error $\bar{\epsilon}_{i,j}$.

(1) w is divided into three bit-streams, L, B, and W using the header file ***head*** which is pre-defined bits from the top of it.

(2) Stretch L to obtain a location map $L_{i,j}$.

(3) Using $B = \{B_1, B_2, \ldots, B_{N_2}\}$, each original pixel $x_{i,j}$ is recovered for $t = 1, 2, \ldots, N_2$, where N_2 is the bit-length of B.

$$x_{i,j} = \begin{cases} \bar{x}_{i,j} - \frac{\bar{\epsilon}_{i,j}}{2} & if\ L_{i,j} = 0 \\ \bar{x}_{i,j} + B_t & if\ L_{i,j} = 1\ and\ \bar{x}'_{i,j} \in S_4 \end{cases} \tag{14}$$

By the *extraction* and *recovery*, both the original image and the watermark are obtained. The flow of the algorithm is depicted in Fig.5

4. Improved Algorithm

In the basic algorithm, a prediction error is first rounded to an even number by expanding itself or by modifying it using Eq.(4). As the detector knows the rule, the calculation of the accurate prediction error is possible in the extraction part. It implies that the information about the formatting is shared with the embedding and the extraction side. If the prediction errors are rounded to even or odd number based on a secret information, eavesdropping of the embedded watermark can be difficult for unauthorized party.

In the Definition 2, a pixel x is modified to x^* in Eq.(4). By introducing the secret information $s \in \{0, 1\}$, the equation is modified as follows

$$x^* = \begin{cases} x - 1 & if\ \epsilon \neq s \pmod 2 \\ x & otherwise. \end{cases} \quad (15)$$

If the secret information is applied for every prediction error, the size is as large as that of an image. In order to reduce the size, we employ a pseudo-random number generator.

Let $x_{i,j}, (0 \leqq i \leqq N-1, 0 \leqq j \leqq M-1)$ be a raster scanned pixel. Then the corresponding secret information bit $s_{i,j}$ is generated from a seed *secret* using the pseudo-random number generator. Based on the above modification, the *formatting* operation is performed as follows.

(1) Calculate the prediction error $\epsilon_{i,j}$ using Eq.(1).

(2) Modify $x_{i,j}$ to $\bar{x}_{i,j}$ based on the following three conditions.

$$\bar{x}_{i,j} = \begin{cases} x_{i,j} + \epsilon_{i,j} + s_{i,j} & if\ x_{i,j} \in S_1 \\ x_{i,j} - 1 & if\ x_{i,j} \in S_2\ and\ \epsilon_{i,j} \neq s_{i,j} \\ x_{i,j} & otherwise \end{cases} \quad (16)$$

(3) If $x_{i,j} \in S_1$, then the location map is set to $L_{i,j} = 0$, else $L_{i,j} = 1$.

(4) If $x_{i,j} \in S_2$, then the LSB of $\epsilon_{i,j}$ is added to a vector $\boldsymbol{B}$ as one element.

After the above formatting, each prediction error is formatted even/odd number dependent on the secret information $s_{i,j}$. Here, the embedding information $\boldsymbol{w}$ can be made from the same component in Eq.8. Then the *embedding* operation is performed based on $s_{i,j}$, and Eq.(10) is modified as follows.

$$\bar{x}'_{i,j} = \begin{cases} \bar{x}_{i,j} + 1 & if\ x_{i,j} \in S_4\ and\ w_t \neq s_{i,j} \\ \bar{x}_{i,j} & otherwise \end{cases} \quad (17)$$

By the above operation, the prediction error becomes even number if $s_{i,j} = 0$, and vice versa.

In the *extraction*, the operations (3-2) and (3-3) in the basic scheme is modified as follows.

(3-2) Re-format $\bar{x}'_{i,j}$ to $\bar{x}_{i,j}$ using the LSB of the prediction error $s_{i,j}$.

$$\bar{x}_{i,j} = \begin{cases} \bar{x}'_{i,j} - 1 & if\ w_t \neq s_{i,j} \\ \bar{x}'_{i,j} & otherwise \end{cases} \quad (18)$$

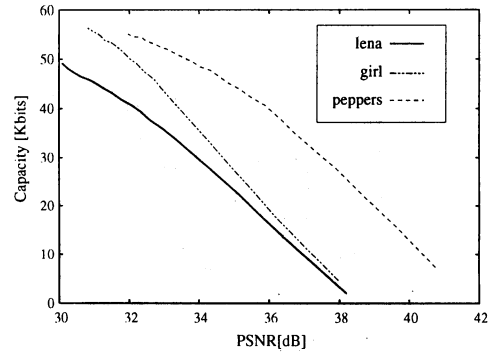

Fig. 6 The capacity of embedding information versus PSNR.

(3-3) Store the re-formatted prediction error $\bar{\epsilon}_{i,j}$.

$$\epsilon_{i,j} = \begin{cases} \bar{\epsilon}'_{i,j} - 1 & if\ w_t \neq s_{i,j} \\ \bar{\epsilon}'_{i,j} & otherwise \end{cases} \quad (19)$$

The recovery of the original image is performed by the same operation as the basic algorithm using the extracted information.

5. Numerical Results

We have been implemented our basic algorithm and estimated the capacity and distortions with basic scheme and the enhanced scheme. The images used in the evaluation are "lena", "girl", and "peppers" with 8-bit gray scale image of 256×256 pixels. The capacity of the watermark information can be approximately expressed by

$$\sigma = N_4 - len(\boldsymbol{head}) - len(\boldsymbol{L}) - len(\boldsymbol{B}), \quad (20)$$

where $len(\cdot)$ outputs the bit-length and N_4 is the number of pixels in S_4. Since $len(\boldsymbol{B})$ is equal to the number of pixels in S_2, Eq.(20) is simply represented as follows.

$$\sigma = N_1 - len(\boldsymbol{head}) - len(\boldsymbol{L}), \quad (21)$$

In the following simulation, the capacity is calculated by omitting the size of ***head*** as it is negligibly small.

First, the capacities obtained by embedding with various threshold T are plotted in Fig.6. The results reveal that the capacity is variable for images. It is because the performance of the predictor in JPEG-LS at a flat region is superior to noisy region in a image, which is dependent on the characteristic of the image.

For the evaluation of the perceptual quality of the watermarked images, both the original and watermarked image are shown in Fig.7 and Fig.8 respectively. Compared with the original image, a kind of sharpening effects is appeared and the effects grow stronger for the increase of the amount of watermark information. If a different secret key is applied for the extraction and recovery operation, the extracted watermark becomes random number and the recovered image is completely collapsed, which is like a sand storm.

Fig. 7 Original image.

Fig. 8 Watermarked image(The capacity is about 40[Kbits] with PSNR 32[dB]).

6. Conclusion

In this paper, a new reversible watermark using the prediction errors calculated in JPEG-LS has been proposed. Since the prediction errors follow TSGD model centered at zero, the distortions caused by our embedding is kept small, and hence the capacity of our basic scheme is rather large. Considering the secrecy of the embedded watermark, a randomization of prediction errors is introduced. Without the secret information, the recovery of both the watermark and the original image is impossible. The future work is to increase the capacity without causing perceptual quality by reducing the size of location map.

Reference

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking,* Artech house publishers, Jan. 2000.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol.14, no.2, pp.253-266, 2005.

[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol.13, no.9, pp.890-896, 2003.

[4] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol.13, no.8, pp.1147-1156, 2004.

[5] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," *IEEE Trans. Image Process.*, vol.9, no.8, pp.1309-1324, 2000.

[6] A. Netravali and J. O. Limb, "Picture coding: a review," *Proc. of IEEE,* vol.68, pp.366-406, 1980.

[7] S. W. Golomb, "Run-length encodings," *IEEE Trans. Inform. Theory,* vol.IT-12, pp.399-401, 1966.