Variance Analysis of Pixel-Value Differencing Steganography

Hao Zhang
Zhengzhou Information Science and Technology Institute
No. 62 Kexue Road, Zhengzhou
Henan Province, China
haozhang78@126.com

Tao Zhang
Zhengzhou Information Science and Technology Institute
No. 62 Kexue Road, Zhengzhou
Henan Province, China
brunda@163.com

Huajin Chen
Zhengzhou Information Science and Technology Institute
No. 62 Kexue Road, Zhengzhou
Henan Province, China
huajin_chen@126.com

ABSTRACT
As the adaptive steganography selects edge and texture area for loading, the theoretical analysis is limited by modeling difficulty. This paper introduces a novel method to study pixel-value difference (PVD) embedding scheme. First, the difference histogram values of cover image are used as parameters, and a variance formula for PVD stego noise is obtained. The accuracy of this formula has been verified through analysis with standard pictures. Second, the stego noise is divided into six kinds of pixel regions, and the regional noise variances are utilized to compare the security between PVD and least significant bit matching (LSBM) steganography. A mathematical conclusion is presented that, with the embedding capacity less than 2.75 bits per pixel, PVD is always not safer than LSBM under the same embedding rate, regardless of region selection. Finally, 10000 image samples are used to observe the validity of mathematical conclusion. For most images and regions, the data are also shown to be consistent with the prior judgment. Meanwhile, the cases of exception are analyzed seriously, and are found to be caused by randomness of pixel selection and abandoned blocks in PVD scheme. In summary, the unity of theory and practice completely indicates the effectiveness of our new method.

CCS Concepts
• Information systems~Data management systems • Security and privacy~Cryptanalysis and other attacks

Keywords
Adaptive steganography; Pixel-value difference; Variance analysis; Least significant bit.

1. INTRODUCTION
A secure steganographic strategy is assumed to use edge pixels [1] or textured area [2] for loading secret message. As these places are difficult to model, the relevant study of theoretical analysis is few and major results have usually been gotten by lots of classification experiments [3]. This paper proposes a novel method for analyzing PVD [4]. Although this edge adaptive algorithm was broken, the idea is still very popular and has been widely improved by people. Some work in recent years refers to Liao [5] and Swain [6]. To establish an effective and universal technique, we consider it significant to start the research from the original algorithm.

Note that the variance or energy of stego noise introduced to cover image, reflects the security of algorithms. The variance statistic is taken as major object for study. The histogram of cover pixel difference plays an important role in PVD scheme, and is considered as parameter. A variance formula is then established seriously through calculating expectation and moment values. In application, we use it to answer an interesting question, whether PVD or LSBM [7] is safer at the same embedding rate. Here, all the results are derived rigorously from theory and also verified by experiments. As is known, the analysis of adaptive schemes in many references relies on experimental observation, and the conclusion is not accurate enough. So the formula method is the characteristic of this article.

The paper is organized as follows. Section 2 describes the symbols by reviewing the embedding process, and makes some essential assumptions. The next two sections give the results of variance formula and security comparison. The final section concludes this study.

2. SYMBOL DESCRIPTION
In PVD scheme, a 256-level grayscale cover image is divided into non-overlapping blocks of two consecutive pixels, by zigzag scan. For each pixel pair (c_0, c_1), the absolute value of difference $d=c_1-c_0$ ranges from 0 to 255. Partition it into six intervals $\{R_k \mid 1\le k \le 6\}$ = {[0,7], [8,15], [16,31], [32,63], [64,127], [128,255]}. Denote the lower and upper bound values of R_k by l_k and u_k, and the interval width by $w_k=u_k-l_k+1$. If $|d|$ belongs to R_k, the block can load with $\log_2(w_k)$ bits. Convert the secret bits into decimal number b. The new difference after embedding will be

$$d_s(b,d)=\begin{cases} l_k+b, & d\ge 0 \\ -(l_k+b), & d<0 \end{cases} \tag{1}$$

Denote the residue for x modulo 2 by $(x)_2$, and the new pixel pair (s_0, s_1) is represented as

$$(s_0,s_1)=\begin{cases} (c_0-r_c(b,d), c_1+r_f(b,d)), & (d)_2=1 \\ (c_0-r_f(b,d), c_1+r_c(b,d)), & (d)_2=0 \end{cases} \tag{2}$$

Here, r_c and r_f are defined by rounding operations:

ICCSP '17, March 17-19, 2017, Wuhan, China

DOI: http://dx.doi.org/10.1145/3058060.3058077

$$\begin{cases} r_c(b,d) = \left\lceil \dfrac{d_s - d}{2} \right\rceil \\ r_f(b,d) = \left\lfloor \dfrac{d_s - d}{2} \right\rfloor \end{cases} \tag{3}$$

$\lceil \cdot \rceil$ is to round towards infinity, while $\lfloor \cdot \rfloor$ is to round towards minus infinity.

The blocks causing falling-off-boundary problem will not be used for loading (See reference [4] for detail). For the sake of brevity, we will ignore the influence of them in theoretical analysis, and correct the computation in numerical experiments.

Before embedding, the scanning sequence will be scrambled according to secret key for security, and so the stego noise will be distributed randomly in image. The secret bit stream is also thought to be random. If a block is selected, then the decimal number *b* is a random variable of uniform distribution:

$$P(b \,\big|\, |d| \in R_k) = 1/w_k, 0 \le b \le w_k - 1 \tag{4}$$

Note that the length of secret bits has close relation to the difference *d*. The embedding capacity $r_{\max}$ in bits per pixel (bpp) can be represented by difference histogram value. Let the probability that $|d|$ belongs to R_k be p_k . Then $r_{\max}$ is computed by

$$r_{\max} = \frac{1}{2} \sum_{1 \le k \le 6} p_k \log_2(w_k) \tag{5}$$

If the embedding rate *r* is smaller than $r_{\max}$, the probability that a block is selected equals to $r / r_{\max}$.

3. VARIANCE FORMULA

Let the cover and stego pixels be *c* and *s*, and then the additive stego noise value is calculated by $n=s-c$. If *c* is selected to load, *n* should be distributed according to equation (4); otherwise, $n=0$. To make the computation brief, we firstly consider the case of maximum embedding. The following two theorems give the expectation $E[n]$ and the second moment $E[n^2]$.

Theorem 1. In the case of maximum embedding, the following equation holds:

$$E[n] = \frac{1}{4} \sum_d (-1)^d P(d) \tag{6}$$

Proof：For any block with the difference *d*, the noise *n* can be computed by equation (2), and *c* is equally likely to be the first or second pixel in the block, thus,

$$\begin{aligned} \mathrm{P}(n = (-1)^d r_c(b,d)) &= \mathrm{P}(n = (-1)^{d-1} r_f(b,d)) \\ &= \frac{1}{2} \end{aligned} \tag{7}$$

From equation (4), we get $E[(b+d)_2 \mid d] = 1/2$. Then we have

$$\begin{aligned} E[n \mid d] &= \frac{1}{2} E[(-1)^d (r_c(b,d) - r_f(b,d)) \mid d] \\ &= \frac{1}{2} (-1)^d E[(b+d)_2 \mid d] \\ &= \frac{1}{4} (-1)^d \end{aligned}$$

Consequently,

$$\begin{aligned} E[n] &= \sum_d P(d) E[n \mid d] \\ &= \frac{1}{4} \sum_d (-1)^d P(d) \end{aligned} \qquad \#$$

Theorem 2. In the case of maximum embedding, the following equation holds:

$$E[n^2] = \frac{1}{48} \sum_{1 \le k \le 6} p_k (12 E_k + w_k^2 + 5) \tag{8}$$

where

$$E_k = \sum_{|d| \in R_k} \frac{P(d)}{p_k} \left(|d| - \frac{l_k + u_k}{2} \right)^2 \tag{9}$$

Proof: With the help of equations (2) and (7), we get

$$\begin{aligned} E[n^2] &= \frac{1}{2} E[r_c^2(b,d) + r_f^2(b,d)] \\ &= \frac{1}{2} \sum_{1 \le k \le 6} \sum_{|d| \in R_k} P(d) E[r_c^2(b,d) + r_f^2(b,d) \mid d] \end{aligned} \tag{10}$$

When $|d| \in R_k$, by using equation (3), we obtain

$$r_c^2(b,d) + r_f^2(b,d) = \frac{1}{2} ((d_s - d)^2 + (d_s - d)_2)$$

Meanwhile, we can get from equation (1) that

$$d_s - d = \begin{cases} l_k + b - |d|, & d \ge 0 \\ -l_k - b + |d|, & d < 0 \end{cases}$$

Thus,

$$r_c^2(b,d) + r_f^2(b,d) = \frac{1}{2} ((l_k + b - |d|)^2 + (b - |d|)_2)$$

Note that *b* follows the uniform distribution (equation (4)). We have

$$\begin{aligned} E[r_c^2(b,d) + r_f^2(b,d) \mid d] &= \frac{1}{2} \sum_{0 \le b \le w_k - 1} P(b) ((l_k + b - |d|)^2 + (b - |d|)_2) \\ &= \frac{1}{2 w_k} \sum_{0 \le b \le w_k - 1} (l_k + b - |d|)^2 + \frac{1}{4} \end{aligned}$$

The first term can be computed by

$$\begin{aligned} &\frac{1}{w_k} \sum_{0 \le b \le w_k - 1} (l_k + b - |d|)^2 \\ &= \frac{1}{w_k} \sum_{0 \le b \le w_k - 1} (l_k - |d|)^2 + \frac{2}{w_k} \sum_{0 \le b \le w_k - 1} (l_k - |d|) b + \frac{1}{w_k} \sum_{0 \le b \le w_k - 1} b^2 \\ &= (l_k - |d|)^2 + (w_k - 1)(l_k - |d|) + \frac{1}{6} (w_k - 1)(2 w_k - 1) \\ &= \left(\frac{l_k + u_k}{2} - |d| \right)^2 + \frac{w_k^2 - 1}{12} \end{aligned}$$

Then we obtain

$$E[r_c^2(b,d)+r_f^2(b,d)\mid d]=\frac{1}{2}\left(|\,d\,|-\frac{l_k+u_k}{2}\right)^2+\frac{w_k^2+5}{24}$$

Finally, put the equation into equation (10), we get

$$\begin{aligned}E[n^2]&=\frac{1}{4}\sum_{1\le k\le 6}\sum_{|d|\in R_k}P(d)\left(\left(|\,d\,|-\frac{l_k+u_k}{2}\right)^2+\frac{w_k^2+5}{12}\right)\\&=\frac{1}{48}\sum_{1\le k\le 6}p_k(12E_k+w_k^2+5)\end{aligned}\qquad\#$$

For any embedding rate $r\le r_{\max}$, equations (6) and (8) should be corrected as follows.

$$E[n]=\frac{r}{4r_{\max}}\sum_d(-1)^d P(d)\qquad(11)$$

$$E[n^2]=\frac{r}{48r_{\max}}\sum_{1\le k\le 6}p_k(12E_k+w_k^2+5)\qquad(12)$$

The value of $r_{\max}$ can be determined by equation (5). Then the variance is gotten by $D[n]=E[n^2]-(E[n])^2$.

We use three standard pictures, listed in figure 1-3, to verify the accuracy of the variance formula. They are all 256 level gray images of 512 x 512 pixels size. The picture 'Lena' has most smooth area, while the picture 'Baboon' has most texture area among them. The influence from abandoned blocks is considered here and the precise capacity values are computed to be 1.551(Figure 1. Lena), 1.587(Figure 2. Man) and 1.698(Figure 3. Baboon).

We conduct the embedding at the rate of integral multiple of 0.1 bpp. Figure 4. shows that the estimation values vibrate closely around the theoretical values for every sample image. This indicates that the variance formula is consistent with the practice, and can always be quite precise, regardless of embedding rate.

4. ALGORITHM COMPARISON

Now, we compare security between PVD and LSBM by the noise variance. The algorithm with a smaller variance will be considered as more difficult to detect, and is safer than the other one. Here, we show that it is not rational to compute the variance directly through the equations (11) and (12). Note that in PVD, each interval has its own modified magnitude. The statistic characters of both pixel region and noise can be rather distinct. To make it reasonable, we should compare the variance in blocks of each interval, respectively. That is to say, we need comparisons for six kinds of region. From the perspective of analysis, if one algorithm performs noisier in a region, then it is easier to be detected in this region. Hence, only when we synthesize all the six results, we can give reliable judgment.

From the proofs of theorems in last section, we know the regional noise variance can be represented as a conditional variance:

$$\begin{aligned}&D[n\,||\,d\,|\in R_k]\\&=E[n^2\,||\,d\,|\in R_k]-(E[n\,||\,d\,|\in R_k])^2\\&=\frac{r}{48r_{\max}}(12E_k+w_k^2+5)-\left(\frac{r}{4r_{\max}}\sum_{|d|\in R_k}(-1)^d\,\frac{P(d)}{p_k}\right)^2\end{aligned}\qquad(13)$$

In LSBM scheme, the embedding strategy for different pixel region is the same, no matter how the difference is distributed. The noise follows the distribution:

$$\begin{cases}P(n=0)=1-\dfrac{r}{2}\\[2mm]P(n=\pm1)=\dfrac{r}{4}\end{cases}$$

And the noise variance in any region should always be $r/2$, Next, we demonstrate that, under some reasonable hypothesis, PVD is proved not safer than LSBM in all regions. As the maximum embedding rate of LSBM is 1 bpp, we restrict the rate r in [0, 1] for fair.

Theorem 3. If $r_{\max}<2.75$, then for any $r\in[0, 1]$ and $1\le k\le 6$, the following inequality holds:

$$D[n\,||\,d\,|\in R_k]>\frac{r}{2}$$

Proof: Note that $r\le r_{\max}<2.75$, $E_k\ge 0$ and

$$\left|\sum_{|d|\in R_k}(-1)^d\,\frac{P(d)}{p_k}\right|\le 1$$

Then we get from equation (13) that

$$\begin{aligned}D[n\,||\,d\,|\in R_k]&\ge\frac{r}{48r_{\max}}(12E_k+w_k^2+5)-\frac{r}{16r_{\max}}\\&>\frac{r(w_1^2+2)}{132}\\&=\frac{r}{2}\end{aligned}\qquad\#$$

As the term E_k defined by equation (9) is abandoned in the proving, the noise variance of PVD is assumed to be much larger than that of LSBM. Here, we use 10,000 images from BOSSbase [8], a popular database in steganographic study, to observe the sample variance in reality, as well as the rationality of the condition. Table 1 show that the capacity ranges from 0.04 to 1.91 and the median and quartiles take values around 1.5. These results imply that most secret bits are loaded by blocks of ranges E_1 and E_2, and the hypothesis "$r_{\max}<2.75$" is pretty reasonable and sufficient. Note that the minimum 0.037 is far smaller than 1. We can also infer that the number of abandoned blocks may be quite large in some images, and the requirement of some embedding rate $r\in[0, 1]$ can not always be met. Consequently, for each statistic, only the samples, which meet the requirement and have blocks of E_k, can be used. It can be seen that the sample number gets smaller while r or k gets bigger. The number is less than 6400 when k=6.

For $k\le 5$, according to the median and quartile values, it is found that the sample variances in pixel region of E_k are mostly larger than $r/2$. When k=1, even the minimum value is bigger than $r/2$. These facts are completely consistent with the conclusion of theorem 3.

Now we explain why there are exceptions for $2\le k\le 6$. We observe those images which create zero value variances. The results state that their blocks of E_k are very few, and the ratio is no more than 1/1000 of total blocks. Moreover, for at least half of these images, the ratio is less than 1/10000. That is to say, the probability the blocks are not selected to load is quite large. In addition, the scheme that abandoned pixels must be eliminated in the selection further reduces this probability. Consequently, the phenomenon is attributed to the randomness of pixel selection in the process of embedding, as well as PVD scheme itself. As a whole, in most images, as well as in most pixel regions, PVD performs noisier than LSBM. So we judge that PVD is not safer than LSBM.

5. CONCLUSION

In this paper, we have established a stego noise variance formula for PVD scheme and analyzed the variance in different pixel region. Note that the experiment results are consistent with our theoretical conclusions. These facts have precisely verified the effectiveness of the proposed analytic technique. We expect that this method can be applied to more adaptive algorithms in the future.

6. ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (No. 61272490 and No. 61572518) and China Postdoctoral Science Foundation (No. 2016M603035). The authors would like to thank the reviewers for their insightful comments and helpful suggestions.

Table 1. Variance statistic for region noise

Statistic		Sample number	Minimum	Lower quartile	Median	Upper quartile	Maximum
Capacity		10000	0.04	1.50	1.52	1.56	1.91
Noise variance for pixel region of E_1	r=0.1	9998	0.08	0.17	0.19	0.21	0.28
	r=0.5	9984	0.43	0.87	0.94	1.04	1.39
	r=0.9	9930	0.77	1.57	1.70	1.88	2.50
Noise variance for pixel region of E_2	r=0.1	9994	0.00	0.17	0.19	0.20	2.14
	r=0.5	9980	0.22	0.89	0.93	0.98	2.38
	r=0.9	9926	0.00	1.61	1.68	1.76	18.00
Noise variance for pixel region of E_3	r=0.1	9975	0.00	0.67	0.72	0.79	40.50
	r=0.5	9961	0.00	3.46	3.63	3.86	21.10
	r=0.9	9907	0.00	6.26	6.55	6.91	84.50
Noise variance for pixel region of E_4	r=0.1	9863	0.00	2.51	2.80	3.17	144.50
	r=0.5	9849	0.00	13.21	14.15	15.37	420.50
	r=0.9	9796	0.00	24.00	25.51	27.45	338.00
Noise variance for pixel region of E_5	r=0.1	9407	0.00	6.75	9.48	12.04	1404.50
	r=0.5	9393	0.00	42.59	50.00	58.88	1404.50
	r=0.9	9343	0.00	79.34	90.87	105.06	1922.00
Noise variance for pixel region of E_6	r=0.1	6349	0.00	0.00	0.00	0.00	739.60
	r=0.5	6336	0.00	0.00	0.00	0.00	1232.67
	r=0.9	6300	0.00	0.00	0.00	0.03	4608.00

Figure 1. Lena.

Figure 2. Man.

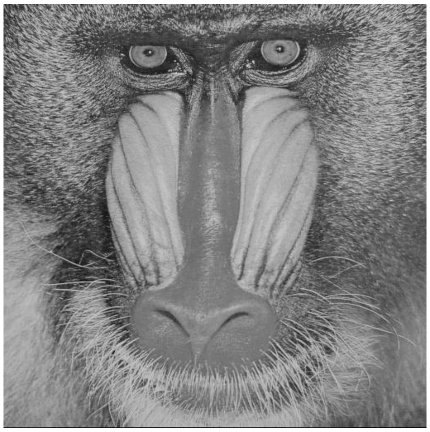

Figure 3. Baboon.

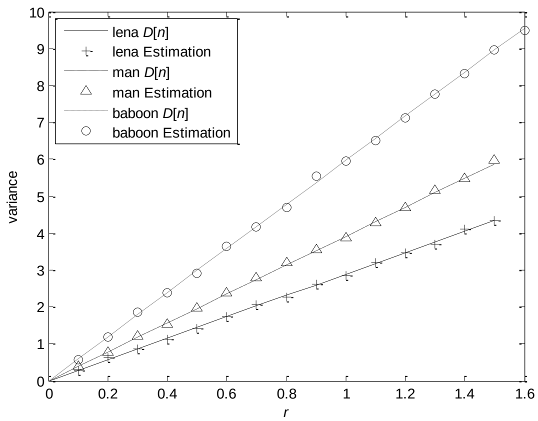

Figure 4. PVD Noise Variance.

7. REFERENCES

[1] Luo, W., Huang, F., and Huang, J. 2010. Edge adaptive image steganography based on LSB matching revisited. *IEEE Tinf. Foren. Sec.* 5, 2 (Feb. 2010), 201-214.

[2] Holub, V. and Fridrich, J. 2012. Designing steganographic distortion using directional filters. In *Proceedings of the IEEE International Workshop on Information Forensics and Security* (December 02-05, 2012), 234-239. DOI= https://doi.org/ 10.1109/WIFS.2012.6412655.

[3] Kodovsky, J., Fridrich, J., and Holub, V. 2012. Ensemble classifiers for steganalysis of digital media. *IEEE Tinf. Foren. Sec.* 7, 2 (Feb. 2012), 432-444.

[4] Wu, D. C. and Tsai, W. H. 2003. A steganographic method for images by pixel-value differencing. *Pattern Recogn. Lett.* 24, 9(Jul. 2003), 1613-1626.

[5] Liao, X. and Ding L. 2015. Data hidng in digital image using four pixel-value-differencing and multiple-base notational. In *Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (September 23-25, 2015), 76-80. DOI=https://doi.org/10.1109/IIH-MSP.2015.28.

[6] Swain, G. and Lenka S. K. 2015. Pixel value differencing steganography using correlation of target pixel with neighboring pixels. In *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies* (March 05-07, 2015), 1-6. DOI=https://doi.org/10.1109/ICECCT.2015.7226029.

[7] Sharp, T. 2001. An implementation of key-based digital signal steganography. In *Proceedings of the 4th Information Hiding Workshop*, *Lect. Notes Comput. Sc.* 2137(Oct. 2001), 13-26.

[8] Filler, T., Pevný, T., and Bas, P. 2010. BOSS (Break Our Steganography System). http://www.agents.cz/boss, July 2010.