Global Journal of Computer Science and Technology: H
Information & Technology
Volume 15 Issue 6 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhancing the Security and Quality Image Steganography using Hiding Algorithm based on Minimizing the Distortion

By Capt. Dr S Santhosh Baboo & V R Sasikumar
Manonmaniam Sundaranar University, India

Abstract- In this paper, highest state-of-the-art binary image Steganographic approach considers the spinning misinterpretation according to the personal visual structure, which will be not secure when they are attacked by Steganalyzers. In this paper, a binary image Steganographic scheme that aims to reduce the hiding misinterpretation on the balance is presented. We excerpt the complement, turn, and following-invariant local balance arrangement from the binary image first. The weighted sum of Complement, Turn, And Following-Invariant Local Balance changes when spinning one pixel is then employed to allot the spinning misinterpretation corresponding to that pixel. By examining on both simple binary images and the composed image constructed message set, we show that the advanced appraisal can well describe the misinterpretations on both visual aspect and statistics. Based on the proposed measurement, a practical Steganographic scheme is developed.

Keywords: binary image, steganography, complement turn, invariant local balance pattern, spinning misinterpretation appraisal.

GJCST-H Classification: H.2.8, I.3.3

ENHANCINGTHESECURITYANDQUALITYIMAGESTEGANOGRAPHYUSINGHIDINGALGORITHMBASEDONMINIMIZINGTHEDISTORTION

Strictly as per the compliance and regulations of:

Enhancing the Security and Quality Image Steganography using Hiding Algorithm based on Minimizing the Distortion

Capt. Dr. S Santhosh Baboo [α] & V R Sasikumar [σ]

Abstract- In this paper, highest state-of-the-art binary image Steganographic approach considers the spinning misinterpretation according to the personal visual structure, which will be not secure when they are attacked by Steganalyzers. In this paper, a binary image Steganographic scheme that aims to reduce the hiding misinterpretation on the balance is presented. We excerpt the complement, turn, and following-invariant local balance arrangement from the binary image first. The weighted sum of Complement, Turn, And Following-Invariant Local Balance changes when spinning one pixel is then employed to allot the spinning misinterpretation corresponding to that pixel. By examining on both simple binary images and the composed image constructed message set, we show that the advanced appraisal can well describe the misinterpretations on both visual aspect and statistics. Based on the proposed measurement, a practical Steganographic scheme is developed. The Steganographic scheme generates the cover vector by dividing the scrambled image into super pixels. Thereafter, the syndrome-trellis code is employed to minimize the designed embedding distortion. Experimental results have demonstrated that the proposed Steganographic scheme can achieve statistical security without degrading the image quality or the embedding capacity.

Keywords: binary image, steganography, complement turn, invariant local balance pattern, spinning misinterpretation appraisal.

I. Introdution

STEGANOGRAPHY, analogous to the message hiding, aims to hide secret knowledge under digital media in such a way that no one, apart from the transmitter and receiver, can detect the existence of the knowledge. In latest years, more message hiding approach have been developed for binary images [1]–[7], which can be used to authenticate digitally stored hand- writings, CAD graphs, signatures, and so on. Stego images obtained by these schemes have also been reported to obtain considerable visual qualities. However, these approaches ignore the safety measure against Steganalyzers. The high undetectability of the secret messages can reduce the suspicion from attackers and thus enhance the safety measure. To this end, we focus on designing a secure binary image message hiding scheme (or more strictly speaking, a Steganographic scheme) by improving the undetectability while preserving the stego image aspect and hiding capacity. Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include Steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for Steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Oftentimes throughout history, encrypted messages have been intercepted but have not been decided. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else.

Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. Essentially, the information-hiding process in a Steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message.

In the spatial region, message bits are generally embedded by directly spinning pixel values in a binary image. Unlike black and white images, pixels in binary images possess only two states: black (1) and white (0). As a reaction, misinterpretations on binary images are easily determined even by personal eyes. To find with this problem, workable Steganographic schemes suggest constraining the hiding to the portions of images that are difficult to be noticed.

Some schemes traced the borderline to find more suitable pixels for hiding message bits [1], [7], whereas the others divided the cover image into overhang/non-overhang blocks and found the best spinning location in each block [2]–[6]. By employing 2 ×2 size blocks and double processing, the scheme

Author α: Associate Professor, P.G and Research Dept. of Computer Science, D.G Vaishnav College, Chennai.
e-mail: vrsasikumar@gmail.com
Author σ: Research Scholar, Manonmaniam Sundaranar University, Tirunelveli. e-mail: santhos1968@gmail.com

Global Journal of Computer Science and Technology (H) Volume XV Issue VI Version I Year 2015

presented in [5] used nearly all the shifted edges to embed message bits and thus obtained a large payload.

Matrix hiding is usually employed to obtain a high hiding efficiency [2], [6], [8] advanced a workable near optimal matrix hiding, namely syndrome-trellis code (syndrome-trellis code), to embed near the capacity misinterpretation bound with respect to the specified misinterpretation appraisal. Prior works also supported the priority of syndrome-trellis code [9]–[11]. Consequently, we employ this code to implement our Steganographic scheme. The above-mentioned schemes all allotment the hiding misinterpretation according to the personal visual structure (hvs).

Therefore, the yielded stego images present good visual qualities and usually cannot be distinguished from the cover images by personal eyes. However, we know that the adversary may reveal the secrets with the assistance of Steganalyzers. As reported in region iv-c, these schemes seem to be insecure in this case.

To make a Steganography scheme secure, an advantage way is to model the image statistic and reduce the hiding impact on that model [9], [12], [13]. Noting that binary images naturally represent the balance [14]–[16], we exploit the balance model to allotment the hiding misinterpretation. broadly speaking, there are three types of approaches describing the balance [17]: geometry-based, statistic-based, and model-based approaches.

In the advanced appraisal, the first and second types are combined to describe the balance with respect to both spatial structure and statistical distribution. That is, we first excerpt the local balance pattern (ltp) as the primary balance. The histogram of ltps is then employed to describe the balance distribution. The ltp is motivated by the concept of the local binary pattern (lbp) [15], [16], which has been successfully applied in balance classification [16], face detection [18], Steganalysis [19], and so on. Since binary images possess different visual appearance compared with black and white images, an extension of the lbp, namely the complement, turn, and following-invariant local balance pattern (complement, turn, and following-invariant local balance), developed to be better applied in binary image Steganography.

We know that the balance region is more suitable for Steganography [10], [20]. Therefore, it is expected that a good stego structure can be obtained in virtue of the balance model. The misinterpretation appraisal needs to coincide with hvs and statistics simultaneously. Unlike the balance-based appraisal advanced, there have been approaches handling misinterpretations by employing the hvs [3], [4], [21], [22]. Among them, wu and liu [3] assessed the spinning misinterpretation according to the smoothness and connectivity in a 3 × 3 window.

Yang and kot [4] defined a connectivity-preserving criterion for 3 × 3 arrangement to determine the flip ability. [21] suggested using the distance reciprocal misinterpretation appraisal to allotment the misinterpretation effect on the neighbouring pixels, and cheng and kot [22] presented an edge line misinterpretation-based criterion to describe the misinterpretation on the borderline connectivity. In this paper, the advanced appraisal is compared with them by using an ifind hiding simulator. In this paper, a spatial region-based binary image Steganography scheme is used.

The scheme reduces a novel spinning misinterpretation appraisal which considers both hvs and statistics. This appraisal employs the weighted sum of complement, turn, and following-invariant local balance changes to allotment the flippability of a pixel. Further, the weight value corresponding to each complement, turn, and following-invariant local balance is set according to that pattern's sensitivity to the hiding misinterpretation. To estimate the sensitivity, a collection of generalized hiding simulators are organized to yield stego images with different misinterpretation types and strengths. In the hiding phase, syndrome-trellis code is employed to reduce the spinning misinterpretation.

To remove the unexpected spinning incurred by syndrome-trellis code, the concepts of scrambling and great pixels are employed to guarantee that flippable elements occupy the majority in a cover vector. By incorporating the new misinterpretation appraisal with the syndrome-trellis code framework, the advanced Steganographic scheme presents a significant performance compared with state-of-the-art works.

The reminder of this paper is organized as follows. The complement, turn, and following-invariant local balance and the spinning misinterpretation appraisal are developed in region ii. In region iii, the advanced Steganographic scheme is presented. Comparison experiments among different misinterpretation appraisals and among different Steganographic schemes are reported in region iv. Finally, region v concludes the whole paper.

II. Spinning Misinterpretation Appraisal

a) *Complement, Turn, and Following-Invariantn Local Balance Pattern*

As a property of areas, the texture involves the spatial distribution of pixels or pixel groups [17]. The invariance against various visual appearances is necessary for a texture descriptor. For example, the gray scale, rotation-invariant local binary pattern technology has been widely employed in texture classification and provided remarkable results [15], [16]. Therefore, we introduce this technique, which is herein named as the local texture pattern (LTP), to our texture model. Binary image processing usually refers to complement, rotation, and mirroring, as shown in Fig. 1. As a result, a local texture pattern which is invariant against these processing, namely a complement, rotation, and mirroring-invariant local texture pattern (crmiLTP), is developed to better fit the application in binary images.

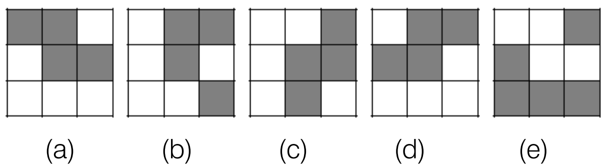


Fig. 1: Demonstration of different binary image processing

Arrangement (b) and (c) are the 45° and 90° rotated versions of pattern (a), respectively. Pattern (d) is obtained by following pattern (a) (i.e., spinning the columns of pattern (a) in the left-right direction) and pattern (e) by inverting pattern (a). According to the advanced complement, turn, and following-invariant local balance. Arrangement (a), (c), (d), and (e) have the same value as 47 while the value of pattern (b) is 61.

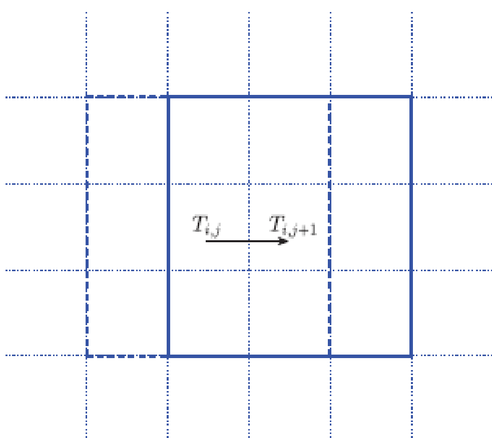


Fig. 2 : One time scanning along the horizontal direction

The LTPs are obtained by scanning the image with a 3×3 size window. Prior work has indicated that, if the scanning step is larger than 2, more interested arrangement cannot be found [4], [7]. Further, the obtained arrangements vary with the location the scanning starts. To guarantee that all the arrangement can be found in both original and shifted/cropped images, the scanning step is set with 1 pixel length, as illustrated in Fig 2. Let the pattern *Ti, j* denote a local neighbourhood of a monochrome balance which is cantered at the location *(i, j)* and covered by a 3×3 size grid. That is

$$T_{i,j} = \{I_c, I_0, I_1, \cdot\ \cdot\ \cdot, I_7\} \qquad (1)$$

Where the pixel Ic denotes the centre pixel of *Ti, j*, and *Ik*, *k* = 0, 1, $\cdot\ \cdot\ \cdot$, 7, denote the 8*L* neighbouring pixels, which are depicted in Fig. 3.

Here in, the white and black pixels are assigned with "0" and "1", respectively. Consider the image complement processing first. Inverting all the pixels in a binary image does not affect the representation of the image content. However, this processing usually changes the balance distribution dramatically, which confuses the LTP-based statistics. As a reaction, the complement invariance is necessary. For this purpose, an exclusive-OR operation is performed on the centre pixel and all the pixels in *Ti, j* to generate the new pattern *T i, j* , written as

$$T_{i,j} = \{I_c \oplus I_c, I_0 \oplus I_c, I_1 \oplus I_c, \cdot\ \cdot\ \cdot, I_7 \oplus I_c\} \qquad (2)$$

2) Counter Clockwise: $I_0, I_7, I_6, \ldots, I_1$

I_0	I_1	I_2
I_7	I_c	I_3
I_6	I_5	I_4

1) Clockwise: $I_0, I_1, I_2, \ldots, I_7$

Fig. 3 : The neighbourhood of *Ti, j*. Neighbouring pixels are labelled with 0, 1. . . 7. These numbers also indicate the scanning sequence used in Eqs. (3) and (4)

Note that the technique in [16] is created to resist arbitrary degrees turn. However, each pixel in a binary image is essentially a black/white square and sensitive to turn, as shown in Fig. 1(b) and (c). As a reaction, we only consider 90 degrees turn invariance, that is, a unique value will be assigned to a pattern and all its multiples of 90 degrees rotated versions. As shown in Fig. 3, there are 8 neigh boring pixels in one 3×3 size pattern, in which adjacent neigh boring pixels are 45° apart. Therefore, the neigh boring pixels are 2-bits-wise rotated in the clockwise direction by 4 times. The value corresponding to each time turn is calculated and the value of *T i, j* is set with the minimal one. Mathematically, the value of *T i, j* traced in the clockwise direction, denoted as $LTP_{ci,j}$, is calculated as..

$$LTP^{c}_{i,j} = \min_{b=0,1,2,3} \sum_{k=0} (I_c \oplus I\,(k+2b) \bmod 8) \times 2^k \qquad (3)$$

The following processing refers to spinning the rows of an image in the up-down direction, or the columns in the left right direction. To obtain the following invariance, we scan the neighbouring pixels in T_{ij} in the counter clockwise direction again, as shown in Fig. 3. Similar to the clockwise direction, these neighbouring pixels are then 2-bits-wise rotated in the counter clockwise direction and the value of counter clockwise traced T_{ij}, denoted as LTP_{ccij}, is set with

$$LTP^{cc}_{i,j} = \min_{b=0,1,2,3} \sum_{k=0} (I_c \oplus I\,(-k-2b) \bmod 8) \times 2^k \qquad (4)$$

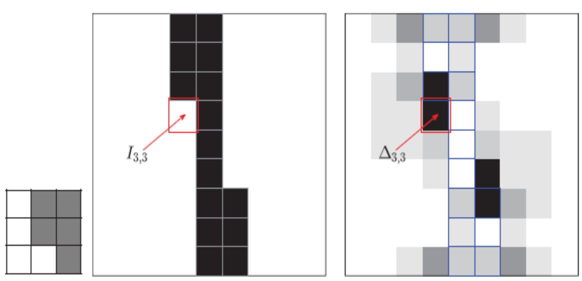
Global Journal of Computer Science and Technology (H) Volume XV Issue VI Version I Year 2015

The final value corresponding to *Ti, j* is assigned with

$$LTP^{crmi}_{i,j} = \min \{LTP^{c}_{i,j}, LTP^{cc}_{i,j}\}$$

As an example, the values of arrangement in Figs. 1(a), 1(c), 1(d), and 1(e) are all equal to 47 after the above calculation, demonstrating the invariance property of the complement, turn, and following-invariant local balance . We know that there have been more extensions to the local binary pattern, such as the multi-resolution and high-dimensional versions [15]. However, experimentally we find that, due to the simple representation of binary images and the lack of samples, these extensions will not offer more advantages and, sometimes, even weaken the performance when they are utilized in binary images.

It is worth noting that prior appraisals presented in [3], [21], and [22] also obtain these invariance properties. Further, the spinning invariance in a binary image has been discussed in [4], [5], and [7] in the perspective of visual aspect. However, in the complement, turn, and following-invariant local balance, the purpose of image processing invariance is to remove the confusions on measuring both visual aspect and statistics.



(a) (b) (c)

Fig. 4. (a) An example of the "l-shape" pattern. (b) A binary image that contains 2 "l-shape" arrangement. (c) The corresponded changing map _. In (c), pixels are represented by squares, of which the black pixels are surrounded by solid lines. The black and white of the square face represents the value of _*i, j*, which varies from 4 to 18. The smaller the _*i, j*, the darker the square face.

b) Definition of Spinning Misinterpretation

A hiding operation that can better preserve an image model is usually more secure [9], [12], [13]. Further, message hidden in the image balance area has been known difficult to be determining [10], [20]. Inspired by these, the advanced spinning misinterpretation function is formed as the detectable hiding changes in the complement, turn, and following-invariant local balance distribution. It can be observed that the change in the number of complement, turn, and following-invariant local balance s when spinning one pixel can loosely indicate the flip ability of that pixel. For instance, it is usually suggested that the best flappable pixels are located at the centre of "l-shape" arrangement (e.g., Fig. 4(a)) [3], [4], [7], [22]. According to the scanning strategy shown in Fig. 2, highest appearances/disappearances of arrangement will be compensated in the next scanning when spinning the centre pixel of a "l-shape" pattern. Let X denote the cover image and $Y_{i,j}$ denote the stego image obtained by only changing the pixel located at *(i, j)*, i.e., $I_{i,j}$, of the cover image X. The change in the number of complement, turn, and following-invariant local balance s when spinning $I_{i,j}$ can be calculated as

$$\Delta_{i,j} = \sum_{t=0}^{255} \left| H_t^{X} - H_t^{Y_{i,j}} \right| \qquad (5)$$

where *H*X and *H* Y*i, j t* are the histogram coefficients corresponding to the complement, turn, and following-invariant local balance s with value equal to *t* which are calculated from images X and Y*i, j*, respectively, computed byl l_w-2l_h-2

$$H_t = \sum_{i=1}^{l_w-2} \sum_{j=1}^{l_h-2} \delta(LTP^{crmi}_{i,j} = t) \qquad (6)$$

where *l*w ×*l*h is the size of the test image and $\delta(\bullet) = 1$ if and only if its argument is satisfied. Take Fig. 4(b) as a simple example. Table I lists all the pattern changing when spinning *I*3,3 in Fig. 4(b). It can be observed that the change in the number of Complement, turn, and following-invariant local balances, _3,3, is only 4. Let the changing map _ consist of _*i, j* as its *(i, j)*-th element. Figure 4(c) depicts the _ calculated from Fig. 4(b). It also indicates that spinning the centre pixels of "*l*-shape" arrangement causes the smallest change, which coincides with the comment from prior works. We now associate the misinterpretation score with the statistical safety measure.

The histogram is a generally employed statistic for the local binary pattern [15], [16], [18], [19]. Further, more workable Steganographic schemes try to offer safety measure by preserving the histogram [12], [13], [24]. A set of cover/stego images are required to evaluate the detection performance of the complement, turn, and following-invariant local balance histogram. To simulate different types of hiding misinterpretations, we construct a generalized hiding simulator, which first assesses each no overhang block and then flips pixels in the selected blocks with a specified probability. Given the *lw* × *lh* size cover image X, the block size l_{sim}, and the spinning probability p_{sim}, the hiding simulator $E_{sim}(X, l_{sim}, p_{sim})$ is performed as follows.

1) Divide X into non-overhang blocks of size $l_{sim} \times l_{sim}$; 2) For each block which is not uniformly white or black, flip each pixel in that block with probability psim; 3) Reconstruct the modified image Y_{sim} and output it. It

can be observed that, the larger the block size l_{sim} is, the more probably the pixel spinning occurs in a uniform region (that is, a region comprised of only white or black pixels). When l_{sim} = 2, all the misinterpretations will be concentrated on the borderline. Herein, we employ the hiding change rate [3]–[5], [25] to describe the hiding misinterpretation on a stego image.

$$\rho\text{sim} = (n_{\text{sim}} \times p_{\text{sim}} \times (l_{\text{sim}})^2) / (l_w \times l_h) \quad (7)$$

The image message set composed in Region A is employed here. By adjusting l_{sim} and p_{sim}, we obtain several sets of stego images with similar misinterpretation strengths but different misinterpretation types. This simulator produces both detectable and undetectable misinterpretations, between which the latter is desired by workable Steganographic schemes. We employ each histogram coefficient as individual feature and estimate its discrimination power on detecting stego images. A histogram coefficient with a large discrimination power indicates that the misinterpretation on the corresponded complement, turn, and following-invariant local balance is easily to be determined. In the hiding phase, we should avoid modifying this histogram coefficient. The optimized Fisher's criterion [26] is employed to evaluate the detection performance of each coefficient in the complement, turn, and following-invariant local balance histogram. the fisher's criterion corresponding to the t-th feature, that is, the histogram coefficient *ht* , can be written as where h_x *t* and hy *t* stand for the histogram coefficients calculated from the cover and stego images, respectively, and $\mu h\bullet_t$ and $\sigma 2h\bullet_t$ represent the mean and variance of $h\bullet_t$.

Since there are 51 histogram coefficients possessing nonzero values, we only depict fisher's criteria corresponding to these coefficients. It can be observed that highest histogram coefficients present fixed performances when altering the hiding types, except those corresponding to the complement, turn, and following-invariant local balances whose values are 1, 2, and 255.

Observing that only a few of complement, turn, and following-invariant local balances present acceptable performances in the previous evaluation, we simply assign nonzero weights to the best 20 complement, turn, and

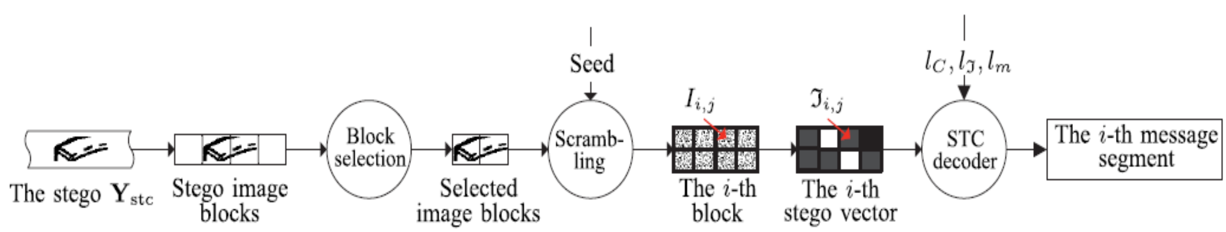


Fig. 5 : The embedding block diagram

following-invariant local balances. The larger the weight is, the more heavily it penalizes the corresponded complement, turn, and following-invariant local balance changing. Finally, the spinning misinterpretation associated with pixel *ii, j* is assigned with the weighted sum of complement, turn, and following-invariant local balance changes, formed as

$$\text{Di,j} = \sum_{t=0}^{255} w_t \; H_t^{x} - H_t^{Y_{i,j}} \quad + \beta \quad (8)$$

Where the α and β can be tuned to control the sensitivity of the misinterpretation score to the borderline structure. They are experimentally set as α = 1/2 and β = 1/2, which can reach the best image aspect. Further, we define the misinterpretation score map D as the matrix that consists of *Di, j* as its *(i, j)*-th element. A Steganographic scheme should only change the pixels with the lowest misinterpretation scores.

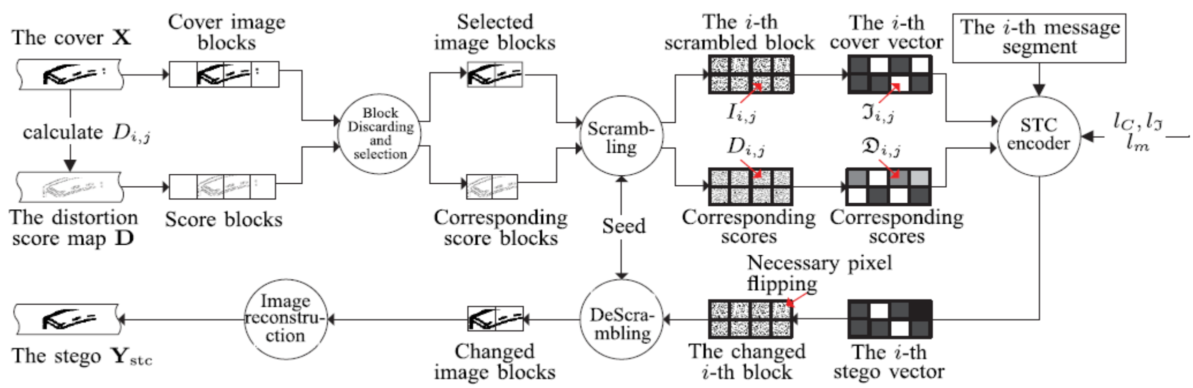


Fig. 6 : The extraction block diagram

III. The Proposed Method

Matrix hiding such as those suggested in [6], [27], and [28] can be employed to reduce the hiding impact on the created misinterpretation appraisal when the payload is given. In [8], a workable optimum code, namely syndrome-trellis code (syndrome-trellis code), is advanced to embed near the payload-misinterpretation bound. The syndrome-trellis code uses the convolutional code with a Viterbi algorithm-based encoder to reduce the additive misinterpretation function. Examples of such approaches as [9]–[11] have also been reported to obtain good performances. Motivated by this, we employ the syndrome-trellis code to implement our Steganographic scheme.

Step 1: image statistics-aware test.

Input: Cover image

Output: Cover image

Action: Overcoming the Spinning Constraint

Given the misinterpretation scores of all the Pixels in an image, syndrome-trellis code are then employed to find the stego vector with the minimum total misinterpretation to finish the hiding. However, the probability of pixels being "wet" (that is, pixels not suitable for spinning) is high in binary images. As a reaction, highest finding of stego vectors in syndrome-trellis code will fail. To find with this problem, the cover image is divided into non-overhang blocks first.

Step 2: Hiding and Excerption Procedure

Based on the advanced misinterpretation appraisal and syndrome-trellis code, the Steganographic scheme is composed in this sub region. It consists of the hiding and excerption procedures, whose block diagrams

Step 3: Hiding Procedure

Input: Pre-processed cover image

Step 4: Calculate the misinterpretation score map of X. Divide the binary message m into non-overhang message segments of length

Step 5: Select all the no uniform blocks in X and the corresponded misinterpretation score blocks in D

Step 6: Consider all the selected blocks in X as an ensemble X and all the selected blocks in D as an ensemble D. Scramble X and D with the same scrambling seed so that each scrambled pixel still corresponds to the correct misinterpretation score at the same location;

Step 7: further divide it into great pixels of size II×II, whose values and misinterpretation scores are calculated

Step 8: for each pixel, whose value needs to be changed, flip the pixel with the lowest misinterpretation score in it;

Step 9: Repeat Steps 5 and 6 until all the message segments have been embedded;

Step 10: descramble the embedded image blocks;

Step 11: successively replace each non-uniform block in the cover image with the corresponded stego block to obtain the stego image Y(syndrome-trellis code).

IV. Experimental Setup

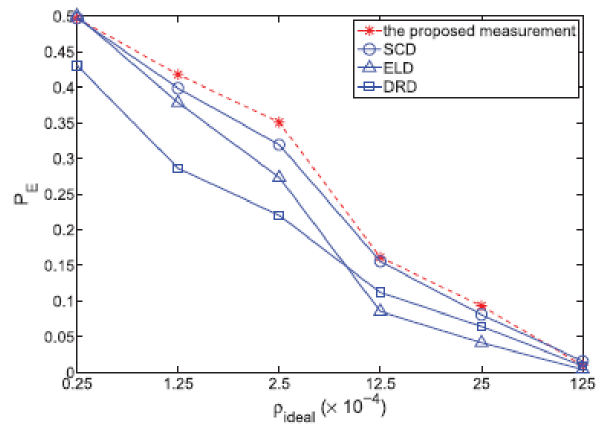
a) Image Message set Setup

It should be noted that these is no generally employed binary image message set, which is necessary to both design a spinning misinterpretation appraisal and evaluate the performance of a Steganographic scheme. In view of this, we detail the setup of the test image message set in this sub region.

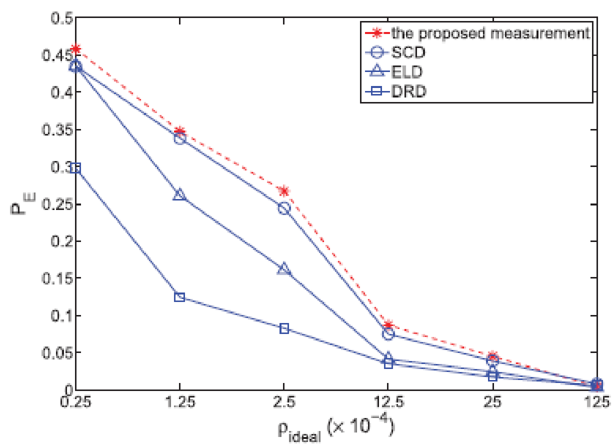
The 5000 original bitmap format binary images used in the experiments consist of "cartoon", "CAD", "balance", "mask", "handwriting", and "document" images. Highest of them are acquired directly from the Google images and [7], except the "balance" images, which are converted from black and white images by thresholding. All the images are cropped into 256 × 256 pixels in order to discard the large blank regions. Some test images are given in Fig. 9. The employed image Sources cover a wide range of contents: the "balance"

Global Journal of Computer Science and Technology (H) Volume XV Issue VI Version I Year 2015

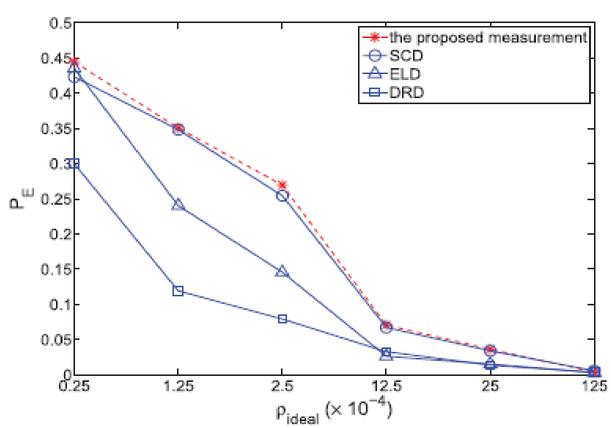
images look noisiest, whereas the "mask" images look smoothest.



(a)



(b)



(c)

Fig. 7 : Safety measure comparison of the i find hiding simulators combined with different misinterpretation appraisals. Utilized steganalytic features are (a) PHD-512D, (b) RLGL-68D, and (c) RLCM-100D

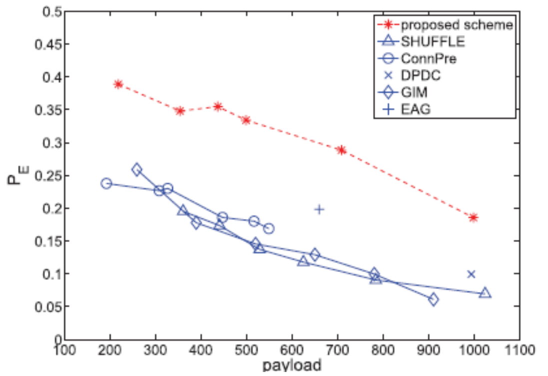
b) Evaluation of the Misinterpretation Appraisal

Unlike in black and white images, hiding message bits in binary images usually causes a serious perceptual misinterpretation. Therefore, the appraisal should well reflect the misinterpretation on the visual aspect besides that on the statistical safety measure. There have been literatures discussing the spinning misinterpretation in binary images [3], [21], [22]. Appraisal suggested in [3] (denoted as SCD) establishes the misinterpretation score by measuring the misinterpretations on both smoothness and connectivity. Appraisal in [21] (denoted as DRD) employs the reciprocal distance to weigh the spinning influences on the neighbouring pixels. In [22], the edge line misinterpretation-based appraisal (denoted as ELD) uses the lengths of edge lines associated with the flipped pixels to allotment the change in the edge similarity. Note that the SCD score is herein defined as 0.625 minus the original value calculated in [3]. In this way, all the appraisals possess the consistent representation: the lower the misinterpretation score, the less the noticeable misinterpretation. Since these appraisals have been generally employed in practice, we compare the advanced misinterpretation appraisal with them to evaluate the performances on both personal visual structure (HVS) and statistics. SCD consider more aspects compared with DRD and ELD, which enhances its sensitivity to statistical misinterpretations. On the other hand, the simple representation of binary images restricts the advantage of the advanced appraisal.

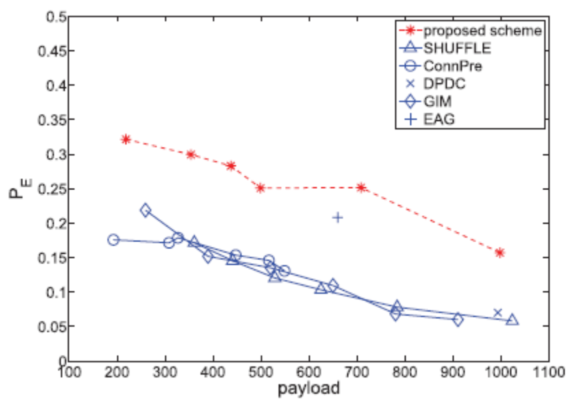
c) Comparison With Other Steganographic Approaches

Some experiments are conducted here to evaluate the advanced Steganographic scheme. The great pixel size it needs to be sufficiently large to guarantee an appropriate probability of each great pixel containing at least one flippable pixel. To better evaluate the performance of the advanced scheme, approaches presented in [3] (denoted as shuffle), [4] (denoted as connpre), [5] (denoted as dpdc), [6] (denoted as gim), and [7] (denoted as eag) are employed for comparison. Shuffle employs the quantization and scrambling to obtain a better image aspect. connpre utilizes the spinning invariant connectivity-preserving arrangement. dpdc uses the interlaced morphological wavelet transform to embed message bits into the shifted edges. GIM proposes a matrix hiding based on the complete set. EAG is edge-based. It proposes a mechanism to employ highest all the "l-shape" arrangement. The scrambling employed in both SHUFFLE and the advanced scheme is implemented by using the Matlab function randperm with a randomly selected seed. In all the experiments, pseudorandom binary sequences are used as messages.

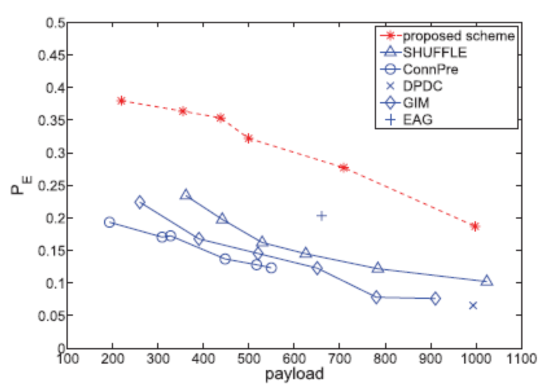
Global Journal of Computer Science and Technology (H) Volume XV Issue VI Version I Year 2015



(a)



(b)



(c)

Fig. 8 : Security comparison of different Steganographic schemes. Utilized steganalyzers are (a) PHD-512D, (b) RLGL-68D, and (c) RLCM-100D

However, we agree that all these schemes have yielded stego images with considerable visual qualities. The adversary may seek the help from steganalyzers to reveal the secret. In view of this, we compare these schemes with respect to the statistical security. The steganalyzers and experiment setup used are still employed here.

Comparison results on the image dataset presented are shown in Fig. 8. It can be observed that the proposed Steganographic scheme achieves the best security. As a result, the proposed scheme can provide additional Steganographic security without degrading the stego image quality.

V. Conclusion and Future Work

In this paper, we exploit the texture property of binary images and propose a secure binary image Steganographic scheme by minimizing the distortion on the texture. The proposed complement, rotation, and mirroring-invariant local texture pattern (crmiLTP) is tolerant of binary image processing and thus can stably describe the local structure of binary image texture. Further, we find that the changes in the crmiLTP distribution show a strong relationship with the detectability of the embedding distortion. Therefore, the proposed flipping distortion measurement is set with the weighted sum of crmiLTP changes, where the weight is empirically assigned according to the discrimination power of the crmiLTP histogram. By comparing with traditional HVS-based approaches, it can be seen that the proposed measurement performs well on both image quality and security. It is worth noting that, employing statistical model to design distortion measurements may raise the risk of embedding in the "clean" edges, which dramatically reduces the Steganographic security in Greyscale images [10]. However, this characteristic provides a reasonable tradeoffs between the image quality and the statistical security in binary images, since distortions not on the boundary are easily to be noticed. At last, a practical Steganographic scheme is constructed by combining the proposed flipping distortion measurement with the syndrome trellis code (STC). Experiments on the constructed image dataset have shown that the proposed Steganographic scheme can yield more secure stego images with better, at least similar, image qualities when the same length of message bits are embedded. In future the crmiLTP and the proposed distortion measurement are extendable for other binary image applications, such as the binary image classification and the assessment of error diffusion methods.

References Références Referencias

1. Q. G. Mei, E. K. Wong, and N. D. Memon, "Message hiding in binary text documents," Proc. SPIE, vol. 4314, pp. 369–375, Aug. 2001.
2. Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure message hiding scheme for binary images," IEEE Trans. Commun., vol. 50, no. 8, pp. 1227–1231, Aug. 2002.

3. M. Wu and B. Liu, "Message hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.
4. H. Yang and A. C. Kot, "Pattern-based message hiding for binary image authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.
5. H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal message hiding for binary images in morphological transform region—A high-capacity approach," IEEE Trans. Multimedia, vol. 10, no. 3, pp. 339–351, Apr. 2008.
6. M. Guo and H. Zhang, "High capacity message hiding for binary image authentication," in Proc. Int. Conf. Pattern Recognit., Aug. 2010, pp. 1441–1444.
7. H. Cao and A. C. Kot, "On establishing edge adaptive grid for bilevel image message hiding," IEEE Trans. Inf. Forensics Safety measure, vol. 8, no. 9, pp. 1508–1518, Sep. 2013.
8. T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive misinterpretation in steganography using syndrome-trellis codes," IEEE Trans. Inf. Forensics Safety measure, vol. 6, no. 3, pp. 920–935, Sep. 2011.
9. T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in Knowledge Hiding (Lecture Notes in Computer Science), R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds., vol. 6387. New York, NY, USA: Springer-Verlag, Oct. 2010, pp. 161–177.
10. V. Holub and J. Fridrich, "Designing steganographic misinterpretation using directional filters," in Proc. IEEE Int. Workshop Inf. Forensics Safety measure, Dec. 2012, pp. 234–239.
11. F. Huang, W. Luo, J. Huang, and Y. Q. Shi, "Misinterpretation function designing for JPEG steganography with uncompressed side-image," in Proc. 1st ACM Workshop Inf. Hiding Multimedia Safety measure, 2013, pp. 69–76.
12. N. Provos, "Defending against statistical steganalysis," in Proc. 10th Conf. USENIX Safety measure Symp., 2001, pp. 323–335.
13. P. Sallee, "Model-based steganography," in Proc. 2nd Int. Workshop Digital Watermarking, 2003, pp. 154–167.
14. B. Wang, X.-F. Li, F. Liu, and F.-Q. Hu, "Color text image binarization based on binary balance analysis," Pattern Recognit. Lett., vol. 26, no. 11, pp. 1650–1657, 2005.
15. D. Huang, C. Shan, M. Ardabilian, Y. Wang, and L. Chen, "Local binary arrangement and its application to facial image analysis: A survey," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 41, no. 6, pp. 765–781, Nov. 2011.
16. T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and turn invariant balance classification with local binary arrangement," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 971–987, Jul. 2002.
17. M. Tuceryan and A. K. Jain, "Balance analysis," in Handbook of Pattern Recognition and Computer Vision, vol. 2. Singapore: World Scientific, 1993, pp. 207–248.
18. A. Hadid, M. Pietikainen, and T. Ahonen, "A discriminative feature space for detecting and recognizing faces," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2. Jun./Jul. 2004, pp. II-797–II-804.
19. Y. Q. Shi, P. Sutthiwan, and L. Chen, "Textural features for steganalysis," in Knowledge Hiding. New York, NY, USA: Springer-Verlag, 2013, pp. 63–77.
20. R. Böhme, "Assessment of steganalytic approach using multiple regression models," in Knowledge Hiding. New York, NY, USA: Springer-Verlag, 2005, pp. 278–295.
21. H. Lu, A. C. Kot, and Y. Q. Shi, "Distance-reciprocal misinterpretation allotment for binary document images," IEEE Signal Process. Lett., vol. 11, no. 2, pp. 228–231, Feb. 2004.
22. J. Cheng and A. C. Kot, "Objective misinterpretation allotment for binary text image based on edge line segment similarity," IEEE Trans. Image Process., vol. 16, no. 6, pp. 1691–1695, Jun. 2007.
23. H. Yang and A. C. Kot, "Binary image authentication with tampering localization by hiding cryptographic signature and block identifier," IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741–744, Dec. 2006.
24. K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Provably secure steganography: Achieving zero K-L divergence using statistical restoration," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 125–128.
25. J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," in Transactions on Message Hiding and Multimedia Safety measure III. Berlin, Germore: Springer-Verlag, 2008, pp. 1–22.

This page is intentionally left blank