Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.163 – 169

RESEARCH ARTICLE

A Novel Steganographic Approach to enhance the Performance of Security System in a Smarter Way

Parveen Mor[1], Tanupriya Choudhury[2], Vasudha Vashisht[3]
[1]Computer Science & Lingayas University, India
[2]Computer Science & Lingayas University, India
[3]Computer Science & Lingayas University, India

[1] parveen.mor439@gmail.com; [2] tanupriya86@gmail.com; [3] ervasudha@gmail.com

Abstract— Steganography can be defined as the process of hiding information by embedding messages within other; Information can be in the form of text, audio, video. Pixel value differencing (PVD) is a steganography method which embeds secret data in images based on spatial information. And to improve the capacity of hiding data is increased by using Tripixel Difference Value Method. In which data is hidden in 2X2 Square block. Here proposed method improves the security of existing TPVD method by making certain modification to make it to more robust to histogram quantization. But it reduces certain capacity of original TPVD algorithm. And the stability of against histogram quantization is significantly improved.

Key Terms: - Steganography; TPVD; PVD; Stego image; Stegnalysis

I. INTRODUCTION

A. *Information Security*

Information security means protecting information and information systems from unauthorized access, use, disclosure, modification, inspection, recording or destruction. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them [1].There are two different ways for securing the information, Cryptography and Steganography.

1) Cryptography

Cryptography is defined as which is used to change the plain text in cipher text or the art of transforming data into a sequence of bits that appears as random and meaningless to an attacker or a side observer.

2) Steganographic

Steganography comes from the Greek Steganos (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds [2Once the secret message has been embedded, it may be transferred across insecure lines or posted in public places.[8]The main purpose of Steganography is to hide a message in another one in a way that prevents any attacker to detect or notice the hidden message. The aim of this work is to develop a new method for hiding message in gray-scale images, mainly embedding text data in digital images.

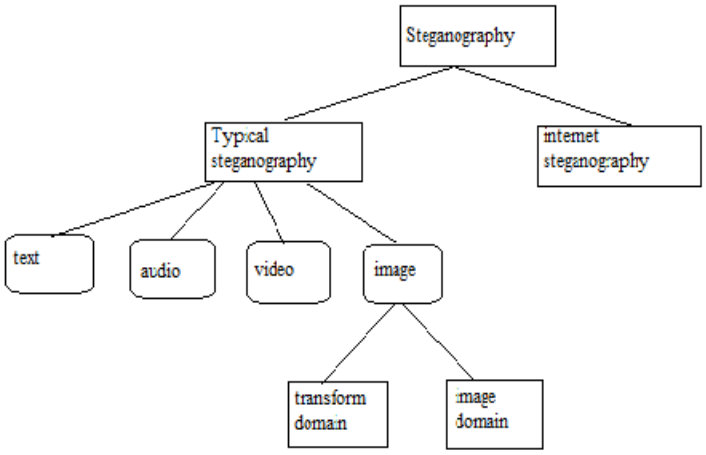


Fig.1 Types of Steganography

B. Types of Steganography

1) Internet Steganography: Internet security is one of the most pressing and difficult problems facing modern private organizations and governments. In addition to the daily barrage of unwanted traffic from network scans, viruses, worms, exploit tools, and other unauthorized attempts to gain access, sites must be concerned with malicious insiders using digital carriers to secretly disperse information through the very perimeter that is supposed to be protecting the network.

2) Typical Steganography: The various types of typical steganography are given below:

- Text Steganography**:** An encoded message just screams you're using encryption, which may attract un-wanted attention to your activities even if snoopers cannot read the text of your messages. Steganography attempts to conceal the presence of an encrypted message; over history a wide variety of techniques have been used: secret compartments in objects, invisible ink, microdots, and grilles used to hide letters of a message among innocent text, and in the digital age, embedding messages as imperceptible noise in images and audio files [3].
- Image Steganography: The purpose of steganography is therefore to hide a secret message in a carrier. And the carrier used to hide the data is any image file that is said to be image steganography [4]. Image based and video based steganographic techniques are mainly classified into spatial domain and frequency domain based methods.. Two important parameters for evaluating the performance of a steganographic system are capacity and imperceptibility. Capacity refers to the amount of data that can be hidden in the cover medium so that no perceptible distortion is introduced. Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading the perceptual quality by data embedding[4]. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, tri-way pixel-value differencing (TPVD) algorithm is used for embedding[7].
- Audio Steganography: Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly [5].
- Video Steganography**:** Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file. The application developed to embed any kind of data (File) in another file, which is called carrier file. The carrier file must be a video file. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds as shown in fig.1.

II. VIDEO STEGANOGRAPHIC ALGORITHM

Here a novel steganographic approach called tri-way pixel-value differencing with pseudorandom dithering (TPVDD) is used for embedding. TPVDD enlarges the capacity of the hidden secret information and provide an imperceptible stego-image for human vision with enhanced security. A small difference value of consecutive pixels can be located on a smooth area and the large one is located on an edged area. According to the properties of human vision, eyes can tolerate more changes in sharp-edge blocks than in smooth blocks. That is, more data

can be embedded into the edge areas than into smooth areas. This capability is made used in this approach which leads to good imperceptibility with a high embedding rate. The Tri-way Differencing Scheme is explained as follows. In general, the edges in an image are roughly classified into vertical, horizontal, and two kinds of diagonal directions. Motivated from the PVD method, using two-pixel pairs on one directional edge can work efficiently for information hiding. This should accomplish more efficiency while considering four directions from four twopixel pairs. This can be implemented by dividing the image into 2×2 blocks and one example block is shown in Figure 2

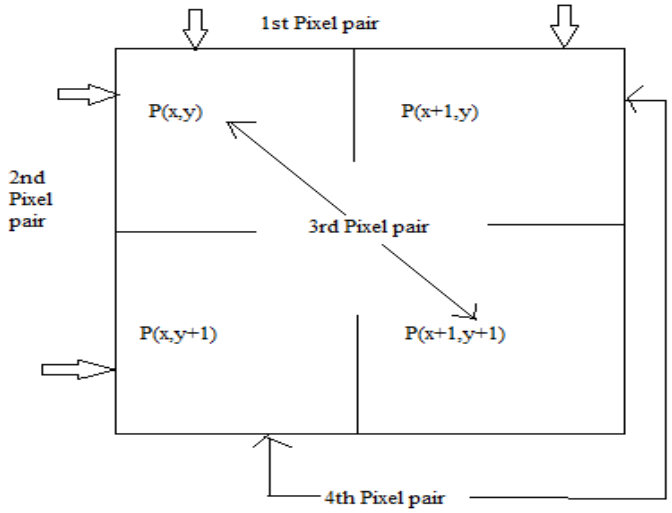


Fig2.An Example of four pixel pair

However, since the changing of pixel values for the fourth pixel pair affects the first and the second pairs, the fourth pair is useless and has to be discarded. Therefore, we propose that three pairs are used to embed the secret data. Before introducing the proposed algorithm, the preprocedure is to partition the cover image into non overlapping 2×2 blocks with 4 pixels. In this scheme, each 2×2 block includes four pixels of $p(x, y)$, $p(x+2, y)$, $p(x, y+2)$, and $p(x+2, y+2)$ where x and y are the pixel location in the image. Let $p(x, y)$ be the starting point, then three pixel pairs can be found by grouping $p(x, y)$ with the right, the lower, and the lower right neighboring pixels. Those three pairs are named by $P0$, $P1$ and $P2$ where $P0= (p(x, y), p(x+2, y))$,$P1= (p(x, y), p(x, y+2))$ and $P2 = (p(x, y), p(x+2,y+2))$ respectively. When using the tri-way PVD method to embed the secret data, each pair has its modified P_i and a new difference value d_i for $i = 0, 1, 2$. Now, the new pixel values in each pair are different from their original ones. That is,we have three different values for the starting point $p(x, y)$ named $p\_0(x, y)$, $p\_1(x, y)$ and $p\_2(x, y)$ from P0, $P1$, and $P2$ respectively. However, only one value for $p\_i(x, y)$ can exist after finishing the embedding procedures. Therefore, one of $p\_i(x, y)$ is selected as the reference point to offset the other two pixel values. That is, two pixel values of one pair are used to adjust the other two pairs and construct a new 2×2 block. Selecting different reference points results in varied distortion to the stego-image. Here, we propose an optimal selection approach to achieve minimum Mean-Square-Error (MSE). Suppose that $mi=d\_i-di$, di and d_i are the difference values of pixel pair i before and after embedding procedures. The rules that can exactly determine one optimal reference pair without really estimating MSE are introduced as follows.

1) If all values of mi are great than 2 or smaller than −2, the optimal pixel pair *ioptimal* is the pair with the greatest $|m|$.

2) If all mi have the same sign and only one mi _ {0,2,-2}, then the optimal pixel pair *ioptimal* is selected from the other two pairs with the smallest $|m|$.

3) If only one mi has a different sign from the other two pairs, the optimal pixel pair *ioptimal* is selected from the other two pairs with the smallest $|m|$.

4) If only one mi _ {0, 2, -2} and the other two mi has different signs, the optimal pixel pair *ioptimal* is the pair with mi _ {0, 1, -1}.

5) If there exists more than one pair with mi _ {0, 2, 2}, the optimal pixel pair *ioptimal* can be selected as any one pair with mi _ {0, 2, 2}.

By following those selection rules described above, we can skip the calculation steps of MSE estimation to obtain the optimal reference pairs. Thus, the total computational complexity can be greatly reduced.

A. *Some Adaptive methods to Reduce Distortion*

Although the proposed approach is feasible for embedding secret data, embedding large amount of bits can still cause serious image distortion easily. Since most distortion is generated from the offsetting process, the following two conditions are further designed to avoid too much offset described by

1) embed _ bit(*P*0)_4 and 1 embed _ bit(*P*1)_6

2) embed _ bit(*P*0)<4 and 2 embed _ bit(*P*0)_8

Where embed_bit(*P*i) represents the total embedding bits along the direction of *P*i. If either one of above two conditions is satisfied, the current block being processed can probably result in higher distortion. Then we use two pixel pairs, *P*0 and*P*3= *P*(*x,y+2*), *P*(*x+2,y+2*)and adopt the original PVD method to individually process those two pairs along one direction. If neither of the conditions is satisfied then PVD is applied to three pixel pairs *P*0, *P*1 and *P*2 in three directions. Here, we name those two conditions as "branch conditions".

B. *Pseudo-random Dithering*

This section describes how pseudo-random dithering is applied the range of pixel differences and further modification for embedding and extraction of secret message.

Step 1: pseudo-randomly select a parameter [0, 1], generated from an embedding key, for each block of two consecutive pixels, and calculate l`k = lk + floor(_.wk) (3)

u`k = lk+1 −1 (4)

where *k* is a range index. Thus, instead of the fixed ranges as used in the original PVD method,the new ranges are defined by the varied *l`k* and *u`k*. In other words, the ranges corresponding to different blocks are differently defined according to a secret key. Because *wk* _ *wk*+1 *u0*

u`k − l`k = lk+1+floor(_.wk+1)−1−lk−floor(_.wk) _ wk−1 (5)

Eqn. (5) indicates that the width of any varied range is no less than that of the original fixed range. If *l`k* _ |*d*| _ *u`k*, a total of log2(*wk*) secret bits are embedded into the corresponding block. Convert the secret bits into a decimal value *b*, and calculate |*e*−*d*| for *d*_0 and mod (*e*, *wk*) = *d d'* = −|*e*−*d*| for *d*<0 and mod (*e*, *wk*) =−*d*

Where *l`k* _ *e* _ *u`k* On the extraction side, b can be restored simply by b=mod(d',wk) (6) Note that if b values in all the blocks are 0, the proposed approach degenerates to the original PVD method and the steps in pixel difference histogram will reveal the presence of hidden data.Nonetheless occurrence of such a case is highly unlikely.

C. *The Embedding Algorithm*

The details of data hiding steps are described as follows.

1)Calculate four difference values *di*,(*x*,*y*) for four pixel pairs in each block given by

d0, (x,y) = P(x+1,y)−P(x,y)

d1,(x,y) = P(x,y+1)−P(x,y)

d2,(x,y) = P(x+1,y+1)−P(x,y)

d3,(x,y) = P(x+1,y+1)−P(x,y+1)

2) Using |*di*,(*x*,*y*)| (*i*=0,1,2,3) to locate a suitable *Rk,i* in the range table designed ,that is to compute *j* = min (*uk* −|*di*,(*x*,*y*)|) where *uk_di* for all 1_*k*_*n*. Then *Rk,i* is the located range.

3) Compute the amount of secret data bits *ti* that can be embedded in each pair by *Rj,i*. The value *ti* can be estimated from the width *wj,i* of *Rj,i*, this can be defined by *ti*=log2*wj,i*.

4) If *ti* of *Pi* (*i*=0,1,2,3) satisfies branch conditions, two pixel pairs *P*0 and *P*3 are processed using original PVD. But new difference *d'i* is to calculate. Otherwise, the proposed tri-way scheme is used to process *Pi*.

5) Read *ti* bits from the binary secret data and transform the bit sequence into a decimal value *bi*.

6) Calculate the new difference value *d'i*,(x,y)

7) Modify the values of *pn* and *pn+1* by the following formula:

(p'n,p'n+1)=(pn−ceil(m),pn+1+floor(m)) (7)

Where (*p*n, *pn*+1) represent two pixels in *Pi* and *m* = (*d'i*−*di*)/2

8) Using the selection rules to choose the optimal reference point *p'i(x,y)* with minimum MSE,then this selected point is used to offset the other two pixel pairs.

9) Now, the new block constructed from all pixel pairs and embedded with secret data is generated.

D. *The Extraction Algorithm*

To retrieve the embedded secret data from the stego-image, the extraction algorithm is described in the following steps.

1) Partition the stego-image into 2x2 pixel blocks, and the partition order is the same as that in the embedding stage.

2) Calculate four difference values *d**i,(x,y) for four pixel pairs in each block given by

d*0,(x,y) = P(x+2,y)−P(x,y)

d*1,(x,y) = P(x,y+2)−P(x,y)

d*2,(x,y) = P(x+2,y+2)−P(x,y)
d*3,(x,y) = P(x+2,y+2)−P(x,y+2)

3) Using $|d^*_i,(x,y)|$ (i=0,1,2,3) locate a suitable $R_{k,i}$. Also find the number of bits t_i that was embedded. If t_i satisfies the branch conditions, two independent pixel pairs are selected.Otherwise, three pixel pairs are used for further processing.

4) The secret message b^* is to calculate for stegoimage is not altered b^* is same as b. Finally b^* is converted to binary to obtain the original secret message.

III. THE PROPOSED STEGANALYSIS METHOD

Growing Anomalies in a test image provides a good estimation of the embedded message rate in that image. Growing Anomalies reaches a constant value after embedding in all possible pixel difference values, and more embedding will not considerably change the calculated value of Growing Anomalies. We have used this property in our proposed steganalysis method. Therefore, it can be claimed the ratio of the Growing Anomalies value of a test image, to the resulted Growing Anomalies value after embedding 100% extra secret message in that image, could be considered as a good estimation of initial secret message rate (SMR)[9].

$$SMR = \frac{\text{Growing Anomalies of test image}}{\text{Growing anomalies after embedding 100\% extra stego image}}$$

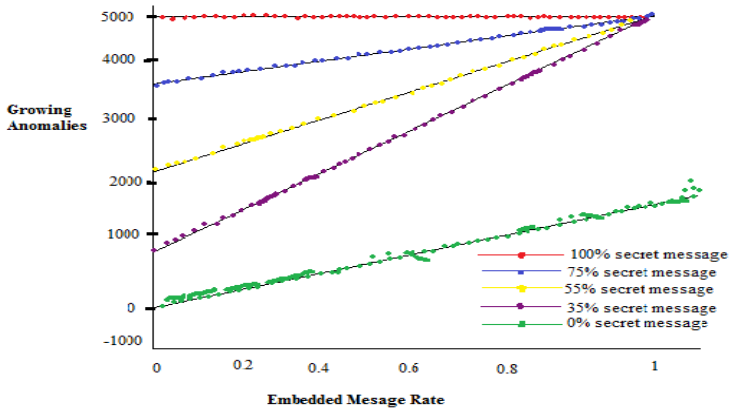
According to Eq. Growing Anomalies value of a test image and its Growing Anomalies value after embedding extra 100% secret data in that image are sufficient to estimate SMR. Also, to enhance the accuracy of our estimation of SMR, a good estimation of those mentioned Growing Anomalies values is needed. If we denote GA(α), α∈ [0,1], as

the Growing Anomalies (GA) value of an image when extra α×100% secret message is embedded in that image, then GA(0) denotes GA value of a test image when no additional extra secret bits embedded in that image, and when extra 100% secret bits are embedded. However, according to our experimental results basically when these distortions appear at GA(0) or GA(1). To understand our solution for this problem, 0.01, 0.02…, 1, for the cover image “Couple” with 0% initial secret message is sketched.

It is obvious that the beginning point of the diagram behaves abnormally comparing to the other points and it can be clearly noticed that Growing Anomalies’ values are decreasing for α=0, 0.01, 0.02..., 0.1. It is apparent that little changes in the value of Growing Anomalies at the starting point will lead to considerable changes in the accuracy of our steganalysis method. To eliminate this unusual behavior, we tried to make use of intermediate values of GA (α=0.01, 0.02, …, 0.99) to estimate GA(0) and GA(1) of a desired test image. To do so, a line P is interpolated regarding all GA(α) points. This line is shown in red in Fig. 3. Instead of starting point and ending point of the GA diagram,P(0) and P(1), are calculated and SMR is computed as Pð0Þ Pð1Þ. Where, P(0) and P(1) are the values of interpolated line P at points 0 and 1 respectively. The estimated SMR for the cover image “Couple” with 0% of initial secret message using Eq. is 8%, but the estimated value of SMR using this new method is about 3%. This assumption is supported by our experimental results on about 150 test images. Then, these features are analyzed and employed by the steganalyser to extract first order polynomial, P, which perfectly fits α values to related GA(α) values (for α=0.00 to 1.00). SMR of that test image. In the final step, SMR is tested by a classifier.

IV. THE EXPERIMENTAL RESULT

First, TPVD steganography is applied on all images and secret data are embedded with different embedding rates including 0%, 35%, 55%, 75% and 100% rate. All cover and resulted stego-images are considered as test images for the second phase.



The proposed steganalysis is applied on all test images. Proposed Steganalysis technique, as mentioned in previous sections. To test the performance of proposed steganalyser, estimated secret message rates are compared with real secret message rates for all test images with different percents of embedded data including 0%, 35%, 55%, 75% and 100%. Average errors are also demonstrated for every group of test images which contain the same message rate. According to these result, the average accuracy of proposed method in estimating secret bits in test images is 97% which shows the effectiveness of proposed Steganalyser in detecting and estimating secret bits under TPVD steganography.

Table 1: Average error for different embedded rates:

Real message rate	Average error
0%	0.090
35%	0.060
55%	0.045
75%	0.028
100%	0.06
Average	0.4

V. CONCLUSION

Tri-way Pixel Value Differencing Steganographic method which is a new modified version of the well-known PVD Steganography technique, is shown to be able to increases PVD's capacity while keeping the visual characteristics of the resulted stego-images. Also, after the introduction of that method in, no effective attack is proposed to reveal existence of hidden data and estimate secret message rate of a stego image under TPVD. However, it is shown here that drastic changes in the probabilistic distribution of pixel pair difference values which have been altered through embedding procedure, hazards the security of TPVD significantly. A new feature named Growing Anomalies (GA) is derived from differences of Tri-way pixel difference histogram. We have proven theoretically and by practical experiences that these GA values follow a regular system and their value has direct relation with embedding rate. We have tested the proposed method on over 150 test images and according to the experimental results, the accuracy of proposed method is 0.97 in estimating secret message rate, with accuracy equal to 0.99 in classifying stego images.

REFERENCES

[1] Donn Parker,Elements of information security,2002.
[2] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image steganography",2002
[3] John walker,"Stego! Text steganography" ,december 2005
[4] Yambern Jina Chanu , Department of Computer Science & Engineering, NERIST, Nirjuli, Arunachal Pradesh, "A Short Survey on Image Steganography and Steganalysis Techniques".
[5] Abdulaleem Z. Al-Othmani, Azizah Abdul Manaf, Akram M. Zeki ,A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation, January 2012.
[6] Sherly A P, Amritha P P , "A compressed Video Steganography using TPVD" ,2010.
[7] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2, JUNE 2008.
[8] Bin Liu, Fenlin Liu, Chunfang Yang and Yifeng Sun "Secure Steganography in Compressed Video bitstreams"
[9] Nazanin Zaker & Ali Hamzeh, "A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram", Springer Science & Business Media, LLC 2011

