Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2014; 2(2B):276-280 **ISSN 2347-9523 (Print)**
©Scholars Academic and Scientific Publisher
(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

An Innovative Approach in Steganography

Sabyasachi Pramanik*[1], Samir K. Bandyopadhyay[2]
[1]Assistant Professor, Haldia Institute of Technology, India
[2]Professor, University of Calcutta, India

***Corresponding author**
Sabyasachi Pramanik
Email: sabyahnt@gmail.com

Abstract: The secure data transmission over internet is achieved using Steganography. In this paper, a new algorithm based on the CPT- has been proposed for data hiding in a image. Here, no is used key for embedding and extracting of data. It hides four bits in a block of size 5×5 by changing a maximum of two bit. Better visual quality can be achieved by the proposed algorithm. The experimental results demonstrate the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality. Simulation experiments show that the proposed watermarking algorithm mis robust and invisible against the common signal processing techniques including JEPG compressing, noise, low-pass filter, median filter, contrast enhance, and the geometric distortions of transpose, mirror reflection, rotation and scale..

Keywords: data transmission, Steganography, JEPG compressing, noise, low-pass filter,

INTRODUCTION

The development in technology and networking has posed serious threats to obtain secured data communication. Since digital multimedia have become progressively advanced in the rapidly growing field of internet application, data securities, including copyright protection and data integrity detection, have become a vast concern. This has driven the interest among computer security [1-2] researchers to overcome the serious threats for secured data transmission. Generally speaking, information hiding [5] relates to both watermarking and Steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand,strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it. One method of providing more security to data is information hiding.Steganography [3] is a branch of information hiding. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) [7] to hide the existence of the message. Steganography is often used in secrete communication. In recent years, many successful Steganography methods have been proposed. This paper represents an innovative approach for embedding [6] four bits in **5X5** block in a image by changing at most two bits with an efficient and invisible way. No key is used here. It should be also consider that Steganography is different from watermarking [4] technique[10].Watermarking is not used to transmit a secret message [8] but to embed data [9], which might be visible, to guarantee ownership.

EXISTING APPROACH

The CPT algorithm [1] is a well-known algorithm applied on a binary cover image to hide data. This algorithm is designed to embed at most **log(ab+1)** bits of the secret message in **a x b** block by the change of maximum two bits.

Here, **K** is the **Secret Key** for embedding & extracting. Its size is **a x b** and it contains **0 & 1**

W is the **Weight Matrix.** It's size is **a x b** and its range is **1 to 2^r –1.**

r is no. of bits embedded in one block.

F is the Cover Image

Embedding Algorithm :

Input: Cover Image **(F),** Secret Key **(K)**, Weight Matrix **(W)** and secret message.

Output: Stego-Image.

Step1: Divide **F** into blocks **(Fi),** each of size a×**b.**

Step2: Determine the size of **r** where **r** $\leq \lfloor$**log(ab+1)** $\rfloor$

Step3: Perform the following steps for each **Fi** until the whole secret message is embedded:

a) Find **(Fi ⊕ K) ⊗W**

b) Find the sum **(s)** of the matrix obtained by the previous step.

c) Find **s** mod **a** where **a=2**^{r}

d) Get the sequence of bits from the secret message.

e) Compare the values obtained from c and d: if they are equal, no action is required, else, one or two bits in **Fi** should be changed to make the values equal.

Extractracting Algorithm :

Input: Stego-image, secret key **(K)** and weight matrix **(W).**

Output: Secret message.

Step1: Divide **F** into blocks **(Fi),** each of size m×n.

Step2: Determine the size of **r.**

Step3: Perform the following steps for each **Fi** until the whole secret message is extracted:

a) Find **(Fi ⊕ K) ⊗W**

b) Find the sum (**s**) of the matrix obtained by the previous step.

c) Find **s** mod **a** where **a=2**^{r} **.** The result is **r** bits of the secret message.

The CPT algorithm can embed **4** bits in a **5×5** block. It uses a secret key and a weight matrix. The proposed algorithm takes a block size **5×5** that can embed **4** bits by changing a maximum of **2** bits as in the CPT algorithm without using a secret key or a weight matrix. It is discussed below-

3. Proposed Algorithm

Here cover image is divided into blocks, each of size **5×5.** In each block, **4** bits from the secret message can be embedded with changing at most two bits in the block.

Embedding Algorithm:

Input: Cover image and secret message
Output: Stego-image.

Step1: Divide the cover image into blocks **(F)** each of size **5×5.**

Step2: For each block, except single-value black and white ones, proceed as follows:

1. For every row in the first four rows of the block, exclusive-or all the bits of that row to get $r_1 r_2 r_3 r_{4.}$

2. For every column in the first four columns of the block, exclusive-or all the bits of that column to get $c_1 c_2 c_3 c_{4.}$

3. Exclusive-or the results in 1 and 2 to get $s_1 s_2 s_3 s_4$ where $s_1 = r_1 \oplus c_1$, $s_2 = r_2 \oplus c_2$, and so on.

4. Compare the result obtained from 3 with the four embedded bits $bit_1 bit_2 bit_3 bit_4$. If there is no difference, no change of bits in **F** is needed, otherwise, consider the following cases:

• if the difference in one bit p_i, the bit $[F]_{i,5}$ or $[F]_{5,i}$ should be changed

• else if difference in two bits p_i and $p_{j,}$ then the bit $[F]_{i,j}$ or $[F]_{j,i}$ should be changed.

• else if difference in three bits $p_{i,}$ p_j and p_k, then the bits

- (($[F]_{i,j}$ or $[F]_{j,i}$) and ($[F]_{k,5}$ or $[F]_{5,k}$)) or
- (($[F]_{i,5}$ or $[F]_{5,i}$) and ($[F]_{k,i}$ or $[F]_{j,k}$)) or
- (($[F]_{5,j}$ or $[F]_{j,5}$) and ($[F]_{k,i}$ or $[F]_{i,k}$))

should be changed

• else (difference in four bits $bit_{i,}$ $bit_{j,}$ bit_k and bit_a) then the bits

- (($[F]_{i,j}$ or $[F]_{j,i}$) and ($[F]_{k,a}$ or $[F]_{a,k}$)) or
- (($[F]_{i,a}$ or $[F]_{a,i}$) and ($[F]_{k,i}$ or $[F]_{j,k}$)) or
- (($[F]_{a,j}$ or $[F]_{j,a}$) and ($[F]_{k,i}$ or $[F]_{i,k}$))

should be changed

The selection of the bit depends on the number of adjacent bits with the same value. The bit that has the least number of adjacent bits is selected. This is because it has a minimum effect on the cover image when it is changed.

Extracting Algorithm :

Input: Stego-Image

Output: Secret message

The algorithm used for extracting is similar to that used for embedding. It performs the following steps to give the embedded data.

Step1: Divide the cover image into blocks **(F)** each of size **5×5.**

Step2: For each block, except single-value black and white ones, proceed as follows:

1. For every row in the first four rows of the block, exclusive-or all the bits of that row to get $\mathbf{r_1 r_2 r_3 r_4}$.
2. For every column in the first four columns of the block, exclusive-or all the bits of that column to get $\mathbf{c_1 c_2 c_3 c_4}$.
3. Exclusive-or the results in 1 and 2 to get the embedded bits $\mathbf{s_1 s_2 s_3 s_4}$ where $\mathbf{s_1 = r_1 \oplus c_1}$, $\mathbf{s_2 = r_2 \oplus c_2}$, and so on.

Example: Say, this is the cover image:

1	1	1	1	1	1	0	0	1	0
1	1	0	0	0	1	0	1	0	1
0	1	0	1	0	0	0	0	0	0
1	0	1	0	0	1	1	0	1	0
1	1	1	1	1	1	1	0	0	0

Data which will be embedded is as follows- **11100101**

Applying the step for every row in the first four rows of the block, exclusive-or all the bits of that row to get $\mathbf{r_1 r_2 r_3 r_4}$ on the given block, and the result is:

1 ⊕ 1 ⊕ 1 ⊕ 1 ⊕ 1 = 1 1 ⊕ 1 ⊕ 0 ⊕ 0 ⊕ 0 = 0 0 ⊕ 1 ⊕ 0 ⊕ 1 ⊕ 0 = 0
1 ⊕ 0 ⊕ 1 ⊕ 0 ⊕ 0 = 0 The result is 1000

Applying the step for every column in the first four columns of the block, exclusive-or all the bits of that column to get $\mathbf{c_1 c_2 c_3 c_4}$ on the same block, and result is:

1 ⊕ 1 ⊕ 0 ⊕ 1 ⊕ 1 = 0 1 ⊕ 1 ⊕ 1 ⊕ 0 ⊕ 1 = 0 1 ⊕ 0 ⊕ 0 ⊕ 1 ⊕ 1 = 1
1 ⊕ 0 ⊕ 1 ⊕ 0 ⊕ 1 = 1 The result is 0011

Applying the step "Exclusive-or the results in 1 and 2 to get the embedded bits $\mathbf{s_1 s_2 s_3 s_4}$ where $\mathbf{s_1 = r_1 \oplus c_1}$, $\mathbf{s_2 = r_2 \oplus c_2}$, and so on" on the same block to get the following result:

1 ⊕ 0 = 1 0 ⊕ 0 = 0 0 ⊕ 1 = 1 0 ⊕ 1 = 1

The result is **1011** and the embedded data is **1110.**

As we can see, the bits number 2 and 4 in the result are different from those in the embedded data. So there should be a
change in either the bit $\mathbf{[F]_{2,4}}$ or $\mathbf{[F]_{4,2}}$**.** Considering its effect on the cover image, the bit $\mathbf{[F]_{4,2}}$ should be changed.
In the other block, if the same operation is repeated, the following results are obtained:

$\mathbf{r_1 r_2 r_3 r_4}$ **= 0101** $\mathbf{c_1 c_2 c_3 c_4}$ **= 0010** $\mathbf{s_1 s_2 s_3 s_4}$ **= 0111**

The embedded data is **0101**.
Therefore, the bit that should be changed is either $\mathbf{[F]_{3,5}}$ or $\mathbf{[F]_{5,3}}$. Based on its effect on the cover image, $\mathbf{[F]_{5,3}}$ is to be changed.

EXPERIMENTAL RESULTS

The proposed algorithm together with the CPT algorithm has been applied on different images for different data.
The following computations were performed for each stego-image:
Similarity: Between the stego-image and the original image

Average: It is computed for each pixel depending on its neighbors. Then the average of pixel average values is also computed to test the consistency between each pixel and its neighbors.

Standard Deviation: Compute the average for each pixel depending on its neighbors, and then compare it with the original image.

The result of Picture1 is shown in Figure 1, Figure 2 and Figure 3 mentioned below.
The comparison between the proposed algorithm and existing CPT algorithm clearly expresses that the proposed algorithm provides a better performance of the Average and Standard Deviation factors but in case of Similarity factor we can see that CPT algorithm offers better result.

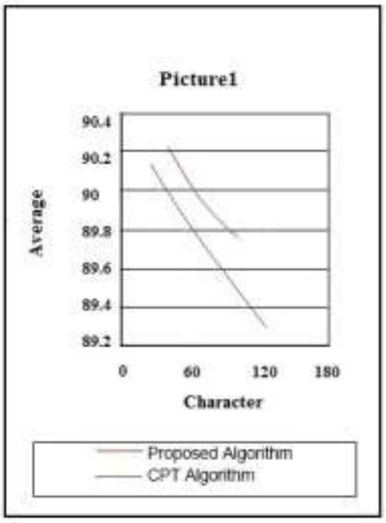

Figure 1 : This is the AverageComparison between Proposed Algorithm and CPT Algorithm

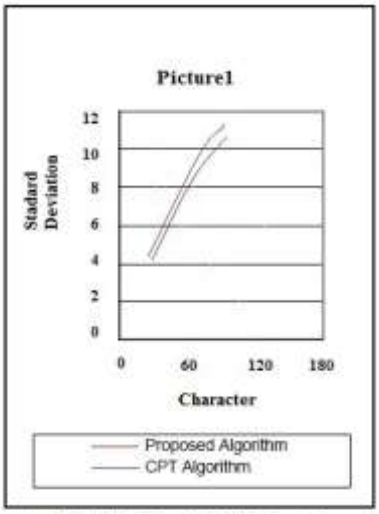

Figure 2 : This is the Standard Deviation Comparison between Proposed Algorithm and CPT Algorithm

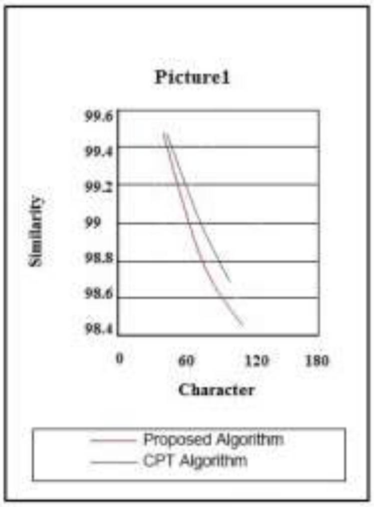

Figure 3: This is the Similarity Comparison between Proposed Algorithm and CPT Algorithm

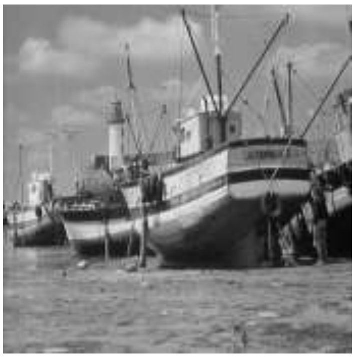

Fig-4(a):The Original Image

Fig- 4(b): The Proposed Algorithm

Fig-4(c):The CPT Algorithm

CONCLUSIONS

In our paper, a new approach has been introduced to hide data in an image. This is an innovative approach in steganography. This Algorithm has some advantages as follows-

- In existing CPT algorithm, key is needed but in this new approach no key is needed only the negotiation between sender and receiver is needed.
- In case of CPT algorithm, the weight matrix is needed to perform the multiplication of the three matrices to calculate the sum**.** This operation takes a huge computational time but the proposed algorithm does not need these computational hazards so time complexity of the algorithm also decreased.
- It shows an improved performance in comparison of average and standard deviations between the original image and stego-image.
- We can also do further improvement of this algorithm by choosing the block randomly rather than choosing it in a sequential way.

REFERENCES

1. Alghoniemy M, Tewfik AH; Geometric invariance in image watermarking. IEEE Trans. On ImageProcessing, 2004;13(2):145-153.
2. Fridrich J, Goljan M, Hogea D; Steganalysis of jpeg images: Breaking the f5 algorithm, Proc. of ACM Workshop on Multimedia and Security 2002, 2002.
3. Fridrich J, Goljan M, Du R; Detecting lsb steganography in color, and gray-scale images ,IEEE Multi Media, 2001; 22-28,.
4. Lu S; Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing, 2005.
5. Lin T, Delp J; A Review of Data Hiding in Digital Images, in Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, 1999; 274-278,
6. Jan Kodovsky, Jessica Fridrich; Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" Proceedings of SPIE, the International Society for Optical Engineering, 2008; 6819.
7. Westfeld A; High Capacity Despite Better Steganalysis (F5-A Steganographic Algorithm)".

Information Hiding. 4th International Workshop. LectureNotes in Computer Science, Vol.2137. Springer-Verlag,Berlin Heidelberg New York, 2001; 289-302

8. Chang CC, Tseng HW; A Steganographic method for digital images using side match. Pattern Recognition Letters, 2004; 25: 1431-1437.
9. Li HF, Chang N, Chen XM; A study on imagedigital watermarking based on wavelet transform. The Journal of China Universities of Posts and Telecommunications, 2010; 17(1):122-126.
10. Westfeld A, Bohme R; Exploiting Preserved Statistics for Steganalysis, in Proceedings of 6th International Workshop on Information Hiding, Canada, 2004; 82-96.