IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver. III (Mar - Apr.2015), PP 12-17
www.iosrjournals.org

An Efficient Data Steganography Using Adaptive Pixel Pair Matching With High Security

Byrapudi Hema Chowdary[1]Aiswariya S[2]Bhavana V[3] Gudapati Srikali[4]

[1] *(Department of ECE, Saveetha School of Engineering Chennai, India.)*
[2]*(Department of ECE, Saveetha School of Engineering Chennai, India.)*
[3]*(Department of ECE, Saveetha School of Engineering Chennai, India.)*
[4] *(Member IEEE, Assistant Professor, Department of ECE, Saveetha School of Engineering Chennai, India)*

Abstract: *Steganography is often outlined as the study of invisible communication that typically deals with the ways in which of hiding the existence of the communicated message.Steganography is nowadays extra vital due to demand of secure communication during this era of vulnerable computer users. The main concept of APPM is to use the pixel pair as a reference coordinate and find a coordinate inside the newly and specially projected compact area set of this pixel pair according to a given message digit.Then that pixel pair gets substituted by the searched coordinate to obscure the digit. It additionally provide adjustable payload and permits users to select digits in any notational arrangement for data embedding, and therefore achieves a larger picture quality. A good data-hiding method ought to be capable of evading discernible and statistical detection as bestowing an adjustable payload. APPM with high security has come to be straightforward, economical embedding method for the data obscuring by removing the assorted shortcomings discovered in the various previous methods established on PPM, such as low-payload problem in EMD. It additionally proposes very less MSE and good PSNR than the OPAP, DE and APPM. High security is provided in this paper by providing an external password along with the secured key. As well as this method is secure below the detection of some well-known steganalysis techniques.*

Keywords*: Adaptive pixel pair matching (APPM), Diamondencoding (DE).Exploiting modification direction (EMD), Optimal pixel adjustment process (OPAP), pixel pair matching (PPM), steganography.*

I. Introduction

Today the expansion within the data technology, particularly in pc networks like internet, Mobile communication, and Digital transmission applications like photographic camera, telephone set, video etc. has opened new opportunities in scientific and business applications. However this progress has conjointly led to several serious issues like hacking, duplications and malevolent usage of digital data. The main aim of steganography is to converse securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to retain others from knowing the hidden data, but it is to retain others from thinking that the data even exists. Alongside the use of steganographic methods, it is probable to obscure data inside digital pictures and video files that is perceptually and statistically undetectable. Steganography is disparate from cryptography in maintaining the secrecy of hidden data in the medium that is utilized for sending the data. Picture steganography uses a digital picture as cover mass media and hence it is called cover image. The data is hidden in the cover picture and the emerging picture is called stego image. The existence of a hidden message in the cover picture is invisible. The embedding of data in a picture can cause distortion in the cover picture and this distortion provoked by data embedding is called embedding distortion. A good data-hiding method ought to be immune to statistical and discernible detection as bestowing an adjustable payload

II. Literature Survey

The most well-known data obscuring scheme is the least significant bits (LSBs) substitution method [1], [2]. This method is easy to apply with low CPU cost, and has become one of the accepted embedding techniques. This method embeds fixed-length hidden bits into the least significant bits of pixels by undeviatingly substituting the LSBs of cover picture with the hidden message bits. Even though this method is easy, it usually results noticeable distortion after the number of embedded bits for every single pixel exceeds three [1]. Countless methods have been counseled to cut the distortion instigated by LSBs substitution

OPAP scheme hunts the negligible distortion value that LSBs equal the embedded bits and replaces stego-pixel value with it [3]. One more method of enhancing LSBs scheme is to cut the number of alterations needed to be introduced into the cover picture for data obscuring after the number of hidden bits is considerably less than that of available cover pixels.

Another method named optimal pixel adjustment procedure (OPAP) method [4] is introduced to reduce the distortion provoked by LSB replacement. In LSB and OPAP methods one pixel is utilized as an embedding unit [5], and hides data into the right-most LSBs. OPAP is conceptually described as matching pixel to its optimal level. OPAP efficiently reduces the picture distortion contrasted with the established LSB method [3]. But in OPAP method, imbalanced embedding distortion emerges and is vulnerable to steganalysis. LSB and OPAP methods are not suitable for applications requiring elevated payload.

Another group of data-hiding methods employs two pixels as an embedding constituent to obscure a message digit **Sb**in b-ary notational system. We word these data-hiding methods as pixel pair matching (PPM). In 2006, Mielikainen [2] counseled an LSB matching method established on PPM. He utilized two pixels as an embedding unit. The LSB of the early pixel is utilized for carrying one message bit, as a binary purpose is retained to carry one more bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel worth has to be modified by one yet one more 1/4 chance no pixel has to be modified. Accordingly, the MSE is $(3/4) \times (1^2/2) = 0.375$ when payload is 1 bpp [2]. In difference, the MSE obtained by LSB is 0.5. In the alike year, Zhang and Wang [4] proposed an exploiting modification direction (EMD) method. EMD improves Mielikainen's method in that merely one pixel in a pixel pair is modified one gray-scale constituent at most and a memo digit in a 5-ary notational arrangement can be embedded. Therefore, the payload is $(1/2)\log_2 5=1.161$bpp. LSB matching and EMD methods considerably enhance the established LSB method in that a better stego picture quality can be attained under the alike payload. However, the maximum payloads of LSB matching and EMD are merely 1 and 1.161 bpp, respectively. Hence, these two methods are not suitable for requests needing elevated payload.

The embedding method of LSB matching and EMD offers no mechanism to rise the payload. In 2008, Hong [6] presented a data-hiding method established on Sudoku solutions to accomplish a maximum payload of bpp. In 2009, Chao et al. [7] counseled a diamond encoding (DE) method to enhance the payload of EMD further. DE employs an extraction function to produce diamond characteristic benefits (DCV), and embedding is completed by modifying the pixel pairs in the cover image according to their DCV's area set and the given message digit. Chao utilized an embedding parameter to control the payload, in that a digit in b -ary notational system can be obscured into two pixels, whereas $b=2n^2+2n+1$.If n=1, b=5 i.e., digits in a 5-ary notational system are obscured, the resultant payload is equivalent to EMD. If n=2, b=13. Note that b is significantly increased as n is merely increased by one. Instead of enhancing the payload of EMD, Wang et al. [8] in 2010 counseled a novel section-wise discovering modification association method to enhance the picture quality of EMD. Their method segments the cover picture into pixel servings, and every single serving is partitioned into the discerning and illustrative groups. The EMD embedding procedure is next gave on every single cluster by referencing a predefined selector and descriptor table. This method combines different pixel clusters of the cover picture to embody more embedding orders alongside less pixel adjustments than that of the EMD method. By selecting the appropriate combination of pixel clusters, the embedding efficiency and the discernible quality of the stego picture is enhanced.

The EMD plan embeds (2n + 1)-ary digit into n spread pixels, however the diamond encoding plan can cover $(2k^2 + 2k + 1)$-ary digit into a spread pixel pair where k is the installing parameter. The point of interest of this plan is depicted as follows.

Assume that a, b, p, and q are pixel qualities, and k is a positive whole number. The area set Sk (p, q) speaks to the set that contains all the vectors (a, b) with the separation to vector (p, q) smaller than k, and Sk (p, q) is characterized as the accompanying structure:

$f(p, q) = ((2k+1) * p+q) \bmod l$

Let absolute value |Sk| indicate the quantity of components of the set Sk, and every part in Skis called neighboring vector of (p, q). We ascertain the estimation of |Sk| to acquire the embedded base and embedded base with a parameter k. Diamond encoding strategy utilizes a diamond capacity f to figure the Diamond Characteristic Value (DCV) in installing and extraction methodology. The DCV of two pixel values p and q can be characterized as follows:

$S_k(p, q) = \{(a, b)|\ |p-a| + |q-b| \le k\}$

Where l is absolute value of Sk. The DCV have two critical properties: the DCV of the vector (p, q) is the individual from Sk fits in with {0, 1, 2, …l,-1} and any two DCVs of vectors in Sk (p, q) are distinct. Expect that Ek speaks to the installed digit and Ek has a place to {0, 1, 2, . . . ,l − 1}. For secret information embedding, we supplant the DCV of the vector (p, q) with the embedded secret digit. Consequently, the modulus distance between f (p, q) and Sk is dk= f (p, q) −Ek mod l. For every k, we can plan a separation design Dk to inquiry which neighboring pixel claims the modulus separation dk. At that point, the vector (p, q) is supplanted with the neighboring vector (p', q') by dk. The vector (p', q') is the individual from Sk (p, q) and the DCV of (p', q') equivalents to the embedded secret digit Ek. The vector (p', q') extract the right secret digit by

$f(p', q') = ((2k+1) \times (p'+ q')) \bmod l$

The diamond encoding plan guarantees that the distortion of vector (p, q) is close to k after embedding a secret digit Ek. Thus, this negligible distortion plan can be utilized to insert substantial measure of information.

This paper proposes a new data embedding method to reducethe embedding impact by bestowing an easy extractionfunction and an extra compact area set. The picture quality obtainedby the counseled method not merely performs larger than those obtainedby OPAP and DE, but additionally brings higher payload withless detectability. Moreover, the best notational arrangement for dataconcealing can be ambitious and retained in this new methodaccording to the given payload so that a lower picture distortioncan be achieved. This method also provides high security by providing an external password along with the internally generated key.

III. Proposed Strategy

3.1.Adaptive Pixel Pair Matching With High Security

APPM is demonstrated to offer security against discovery and lower mutilation however it has further risk of change so the proposed strategy will take forward APPM for grayscale pictures with better security and lower distortion. The PPM-based system, assume a digit TB is to be covered. The scope of TB is around 0 and B-1, and a co-ordinate (p', q') in Ø (p, q) must be discovered such that f (p', q') = TB· [1] Therefore, the range of (p, q) must be numbers somewhere around 0 and B-1, and every number must happen at any rate once. Moreover, to decrease the distortion, the number of co-ordinates in Ø (p, q) ought to be as little as would be prudent. The best PPM technique should fulfill the accompanying three necessities:

1) There are precisely B co-ordinates in Ø (p, q) [[1]

2) The estimations of extraction functions in these co-ordinates are totally unrelated. [1]

3) The configuration of Ø (p, q) and f (p, q) ought to be equipped for inserting digits in any notational framework so that the best can be chosen to attain to lower embedding distortion. [1]

3.2 Extraction Function And Neighborhood Set

The definition of Ø (p, q) and f (p, q) essentially influence the stego picture quality. The design of Ø (p, q) and f (p, q) need to satisfy the accompanying prerequisites:

a) All qualities must be fundamentally unrelated and the summation of the squared separations between all directions in Ø (p, q) and f (p, q) must be the smallest. [1]

b) This is on the grounds that, inserting, (p, q) is replaced by one of the co-ordinates in Ø (p, q) [1]

c) Suppose there are B co-ordinates in Ø (p, q) i.e., digits in a B-ary notational framework are to be hidden, and the likelihood of supplanting (p, q) by one of the co-ordinates in Ø (p, q) is identical. [1]

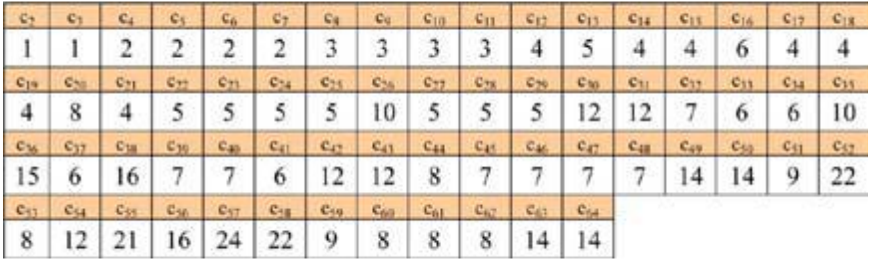
d) The mean of MSE can be obtained by averaging the summation of the squared separation between and other co-ordinates in Ø (p, q)). Hence, given an Ø (p, q) the expected MSE can be ascertained by

$$MSE_{\emptyset(p,q)} = \frac{1}{2}\sum_{i=0}^{B-1}\{(p_i - p)^2 + \ (q_i - q)^2\}$$

The solution of Ø (p, q) and f (p, q) is undoubtedly a discrete optimization problem

$$\begin{aligned} subject\ to{:}\ & f(p_i, q_i) \in \{0,1, \dots\dots\dots, B-1\} \\ & f(p_i, q_i) \neq f(p_j, q_j)\ if\ i \neq j \\ & for\ 0 \leq i, j \leq B-1 \end{aligned}$$

$$minimize{:}\ \sum_{i=0}^{B-1}\{(p_i - p)^2 + \ (q_i - q)^2\}$$



c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4	4
c_{19}	c_{20}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}	c_{27}	c_{28}	c_{29}	c_{30}	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
4	8	4	5	5	5	5	10	5	5	5	12	12	7	6	6	10
c_{36}	c_{37}	c_{38}	c_{39}	c_{40}	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	c_{46}	c_{47}	c_{48}	c_{49}	c_{50}	c_{51}	c_{52}
15	6	16	7	7	6	12	12	8	7	7	7	7	14	14	9	22
c_{53}	c_{54}	c_{55}	c_{56}	c_{57}	c_{58}	c_{59}	c_{60}	c_{61}	c_{62}	c_{63}	c_{64}					
8	12	21	16	24	22	9	8	8	8	14	14					

Table 1. List of constant C_B for 0≤B≤64

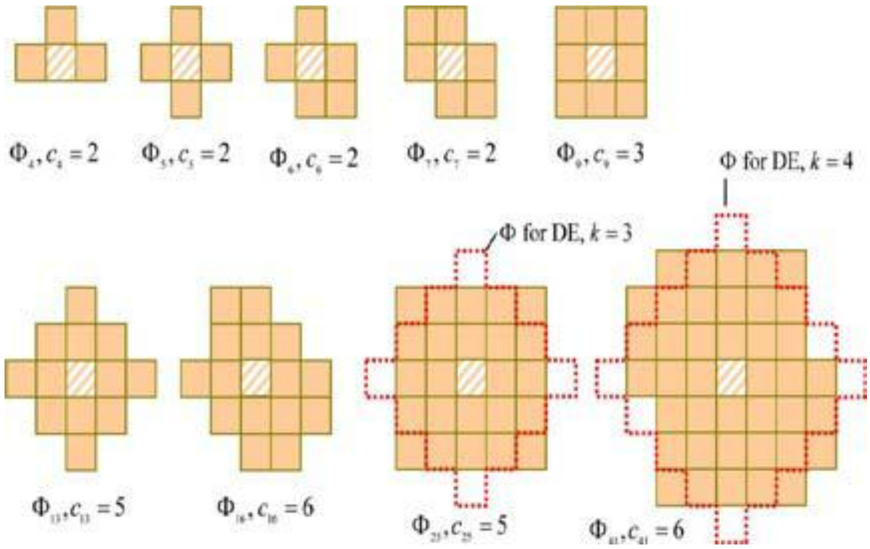


Figure 1. Neighborhood set for APPM

3.3 Embedding Procedure

Here the secret information must be embedded into the given cover picture. For this first we ought to ascertain the picture size and message size. On the off chance that the message size exceeds size of the picture, then the installing methodology isn't possible.

Consider the picture estimate as MxM, For S message bits the size of secret message S is |S|. By utilizing these, calculate the minimum B esteem such that all the message bits can be inserted. The message digits will be consecutively concealed into sets of pixels.

1. Calculate minimum B fulfilling $[M \times M/ 2] \geq |S_B|$
2. Convert the secret message S in to the arrangement of digits with a B-ary notational framework $S_{B.}$
3. Find out c_B and $Ø_B$ (p, q) by solving the discrete optimization problem.
4. From the region characterized by $Ø_B$ (0, 0) record the co-ordinate $(\hat{p}_i, \hat{q}_i)$ such that $f(\hat{p}_i, \hat{q}_i) = i$, $0 \leq i \leq B-1$.
5. Construct a non-repeating irregular embedding succession Q utilizing a key Kr.
6.To embed a message digit S_B, two pixels (p, q) in the cover picture are chosen as indicated by the embedding succession Q, and compute the modulus separation $d=(s_B - f(p,q)) \bmod B$ between s_B and f(p,q), then supplant (p, q) with $(p+\hat{p}_d, q+\hat{q}_d)$.
7. Create an external password to provide high security to the hidden secret message.
8. Repeat step 6 until all the message bits are disguised.

3.4 Extraction Procedure

To get the embedded message digits, pixel sets are examined in the same order as done in the embedding method. The values of extraction function of a checked pixel pair gives the embedded digit.

1. Generate the embedding sequence using the key K_r.
2. Take two pixel positions (p', q') based on the embedding sequence Q and the value of f (p', q') is the embedded digit.
3. Repeat step 2 until all the message digits are extracted.
4. The decimal estimation of these extracted message digits are converted into a binary bit stream to get message bits S.
5. Finally the secret message from the stego image are obtained by providing the internally generated key as well as the external password.

IV. Results

In our experiment, the quality of the stego-image is measured by the peak signal-to-noise ratio (PSNR). The PSNR is the most popular criterion to compute the distortion between the cover picture and stego-image.∑

It is described as follows:

$$PSNR=10 \times \log_{10}(255^2/MSE)$$

Where MSE is the mean square error between the cover picture and stego-image:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Here, the signals I (i, j) and K (i, j) represent the pixel benefits of the cover picture and stego-image in the locale (i, j) respectively, and m and n are the width and height of the original image.
The obtained values from our method are

Table 2.psnr values

IMAGE	PSNR
Lena	53.2935
Baboon	53.2888
Cat	53.3166
bird	53.3208

The stego images are as shown below

figure (a) stego image of Lena

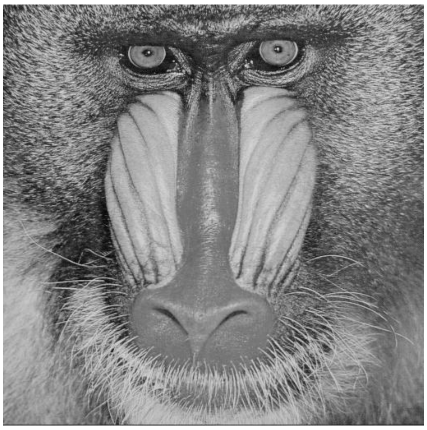


figure (b) stego image of baboon

figure(c) stego image of cat

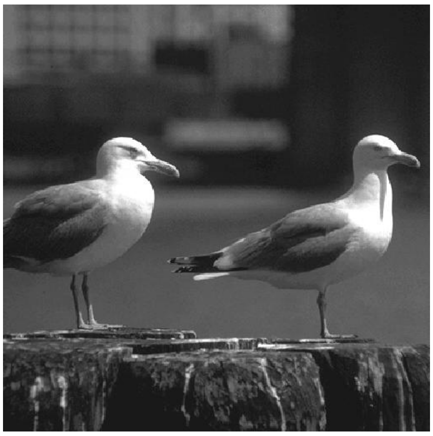


figure (d) stego image of bird

V. Conclusion

This paper is an efficient data steganographic scheme established on the adaptive pixel pair matching provided with high security. In this paper we provided high security by giving an external password along with the internal key so that the secret message is secured among the communicating parties. This method has been utilized to alleviate distortions after embedding a hidden digit into two cover pixels by providing good psnr value.It not merely keeps elevated stego-image quality but additionally conceals colossal amount of data into cover pictures for hidden communication. The presentation of the counseled scheme proves to be better than the easy LSB method and supplementary continuing schemes in words of payload and stego-image quality.

References

[1]. Wien Hong and Tung-Shou Chen, “A Novel DataEmbedding Method Using Adaptive Pixel Pair Matching”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, February 2012.

[2]. J. Mielikainen, “LSB matching revisited,” IEEE Signal Process. Lett. vol. 13, no. 5, pp. 285–287, May2006.

[3]. C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit. vol. 37, no. 3, pp. 469–474, 2004.

[4]. X. Zhang and S. Wang, “Efficient steganographic embedding by exploiting modification direction,”IEEE Commun. Lett. vol. 10, no. 11,pp. 781–783,Nov. 2006.

[5]. A. D. Ker, “Steganalysis of LSB matching in grayscale images,” IEEE Signal Process. Lett. Vol.12, no. 6, pp. 441–444, Jun. 2005.

[6]. W. Hong, T. S. Chen, and C. W. Shiu, “A minimal Euclidean distance searching technique for Sudoku steganography,” in Proc. Int. Symp.Information Science and Engineering, 2008, vol. 1, pp. 515–518.

[7]. R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, “A novel image data hiding scheme with diamond encoding,” EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[8]. J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, “An improved section-wise exploiting modification direction method,” SignalProcess., vol. 90, no. 11, pp. 2954–2964, 2010.