

Data Hiding Technique using Adaptive Pixel Pair Matching

Teena Thomas¹ Chithira P R²

¹Student, M. Tech ²Assistant Professor, Communication Engineering

^{1,2}Electronics and Communication Department, FISAT

Abstract--- In the new era of wireless communication and developing information security techniques, it is very necessary to maintain security of images which serve as a source for data analysis for different applications. Therefore there is rapid demand for reliable techniques, to ensure the security of images. This proposed technique discusses the implementation of a new data hiding technique based on adaptive pixel pair matching. The proposed technique uses the chaotic map based encryption to increase the rank of security in case of attacks.. The basic idea of PPM is to use the pixel pair values as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair based on a given message digit.

Keywords: Adaptive Pixel pair matching, PPM

I. INTRODUCTION

Cryptography was developed as a technique for securing the secrecy of communication and various methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography (Data Hiding). The strength of steganography can thus be increased by combining it with cryptography. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are called cover images and images with data embedded as stego images. After embedding, pixels in the cover images will be modified and there will be distortion occurs. The distortion occurs during data embedding is called the embedding distortion.

The proposed method offers lower distortion when compared with Diamond Encoding [2] DE by providing more compact neighbourhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP)[4] method, the proposed method always has lower distortion for different payloads. The proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well-known data hiding techniques.

Chaotic map [3] based encryption is done in order to increase the security. Here in this paper, a steganographic algorithm using adaptive pixel pair matching is proposed for the embedding and extraction of text.

II. EXTRACTION FUNCTION AND NEIGHBOURHOOD SET

This method is a new data embedding method to reduce the

Embedding impact by providing a simple extraction function and a more compact neighborhood set [1]. This method embeds more messages per modification and thus increases embedding efficiency. Moreover, the best notational system for data hiding can be determined and employed in this method so that a lower image distortion can be achieved.

An adaptive pixel pair matching (APPM)[1] data-hiding method has better $f(x, y)$ and $\Phi(x, y)$ so that MSE is minimized. Data is then embedded by using PPM based on this $f(x, y)$ and $\Phi(x, y)$.

$$f(x, y) = (x + C_B * y) \text{ mod } B \tag{1}$$

C_B is a constant

The solution of $\Phi(x, y)$ and $f(x, y)$ is indeed a discrete optimization problem.

$$f(x_i, y_i) \in \{0, 1, \dots, B-1\} \tag{2}$$

$$f(x_i, y_i) \neq f(x_j, y_j) \text{ if } i \neq j \tag{3}$$

For $0 \leq i, j \leq B-1$

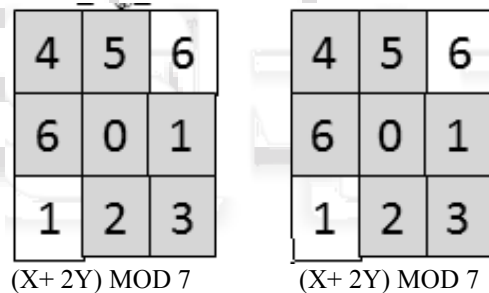


Fig. 1: Neighborhood set for Different C_B values

A. Embedding Algorithm

Input: Cover image I of size MxM, secret bit stream S, and key.

Output: Stego image I', C_B , and $\Phi_B(x, y)$.

Step1. The cover image is encrypted using Chaotic maps
 Step2. Find the minimum B satisfying, $\lceil \frac{M \times M}{2} \rceil \geq S_B$ and convert S into a list of digits with a B -ary notational system S_B .

Step3. Solve the discrete optimization problem to find C_B and $\Phi(x, y)$.

Step4. In the region defined by $\Phi_B(0,0)$, record the coordinate (x_i, y_i) such that $f(x_i, y_i) = i, 0 \leq i \leq B-1$.

Step5. Construct a nonrepeat random embedding sequence Q using a key.

Step6. To embed a message digit S_B , two pixels in (x, y) the cover image are selected according to the embedding sequence Q, and calculate the modulus distance $d = (S_B - f(x, y)) \text{ mod } B$ between S_B and $f(x, y)$, then replace (x, y) with $(x + xd, y + yd)$.

Step7. Repeat Step 5 until all the message digits are embedded.

B. Extraction Algorithm

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

Input: Stego image I' , C_B , and $\Phi_B(x,y)$.

Output: Secret bit stream S .

Step1. Construct the embedding sequence Q using the key

Step2. Select two pixels (x',y') according to the embedding sequence Q .

Step3 Calculate $f(x',y')$, the result is the embedded digit.

Step4. Repeat Steps 2 and 3 until all the message digits are extracted.

Step5 Decrypting the image to get original cover image

Step6. Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream.

III. PROPOSED TECHNIQUE

The cover image of size 256×256 is taken. If the image is colour its gray scale image plane will be chosen for encryption. The resultant image is encrypted using chaotic maps[3]. The data hiding is done by using adaptive pixel pair matching. Finally the data can be extracted from stego image. This can be explained in the below figure.

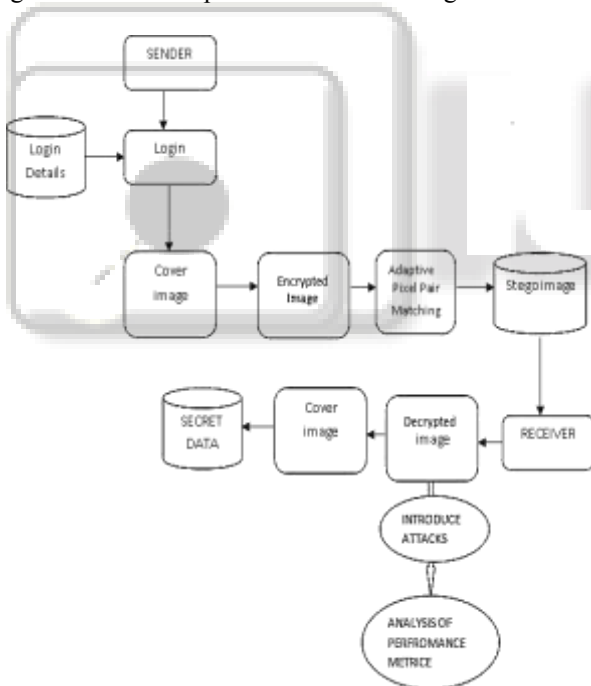


Fig.2. Block Diagram of Proposed Technique

IV. ENCRYPTION OF COVER IMAGE

The approach is that before the text files are being embedding to the cover image, the entire image is encrypted using chaotic maps. After extracting the data, the image is decrypted back to original image.

Chaotic map is defined as

$$X_{n+1} = \lambda \times X_n \times (1 - X_n) \quad (4) \quad \lambda \in$$

$(0,4) \quad n=0, 1, 2, \dots$

The parameter λ and initial value X_0 may represent the key.

V. RESULTS

In the simulation process two phases are there. First the image is encrypted using chaotic maps and then data is embedded. After the data embedding we can extract the data and finally we get the decrypted image.

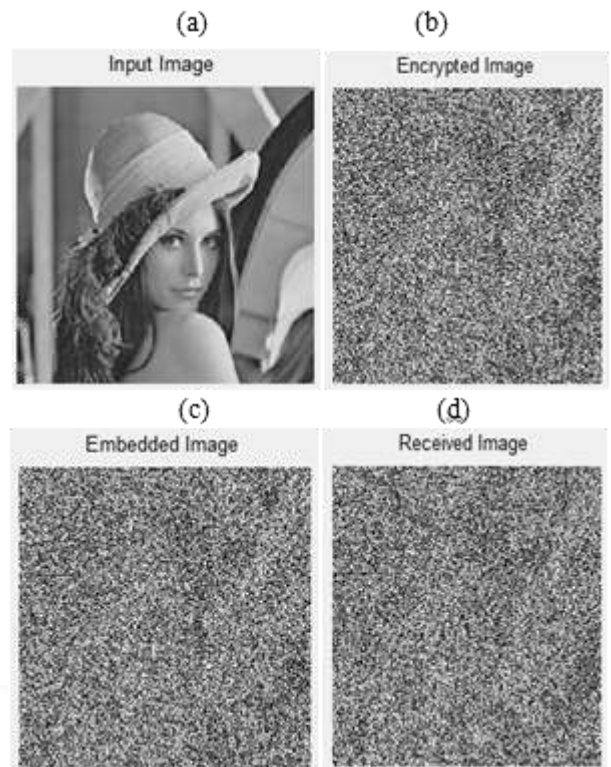


Fig. 3: (a) Input Image. (b).Encrypted Image.(c).Embedded Image .(d).Received Image



Fig. 4: Decrypted Image

Finally the secret data is extracted from the image.

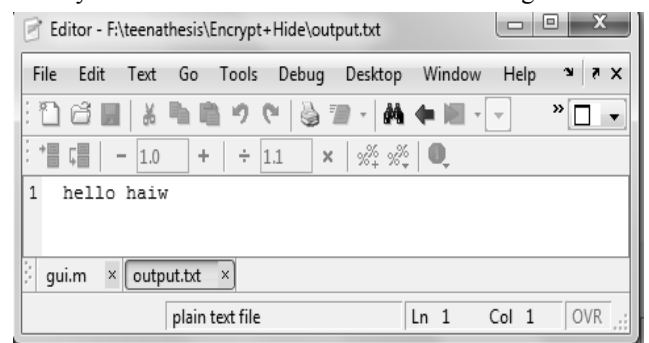


Fig. 5: secret data

VI. CONCLUSION

With the new multimedia and wireless communication it is very necessary to maintain image security which serves as a source for critical data analysis. A new data hiding technique was implemented which is based on adaptive pixel pair matching. Also using a layered approach by combining cryptography and data hiding adds to the rank of security of the image. A chaotic based encryption increases the level of security. The image quality after implementation of the new technique was found to be good, with no loss of data. Thus it can be concluded that the Data hiding can be done in the adaptive pixel pair matching preserve the image quality and for security.

ACKNOWLEDGEMENT

We would like to extend heartfelt and sincere gratitude to Wien Hong, the author of "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", 2012 IEEE, for his technical and moral guidance. His paper on "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching" was very insightful which acted as the backbone structure for this paper.

REFERENCES

- [1] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching". IEEE Transactions on Information Forensics and security, VOL. 7, NO. 1, FEBRUARY 2012.
- [2] Ruey-Ming Chao,¹ Hsien-ChuWu,² Chih-Chiang Lee,³ and Yen-Ping Chu⁴, Research Article "A Novel Image Data Hiding Scheme with Diamond Encoding", EURASIP Journal on Information Security Volume 2009
- [3] Muhammad Usama, Muhammad Khurram Khan, Classical and Chaotic Encryption Techniques for the Security of Satellite Images, IEEE conference on computing science.2008
- [4] Rajashree Shitole, Satish Todmal: A novel image hiding scheme by Optimal Pixel Pair Matching and Diamond Encoding, IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 1 issue 5 january2013.