INVESTIGATION OF ALGORITHMS FOR REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES/MULTI OBJECT DETECTED IMAGES

Mr. N. V Shibu[1], Ahamed Hussain K[2], Eniyadharsan D[3], Kannan T[4]

1 Professor & Head of the Department, Department of Computer Science & Engineering, Sri Ramakrishna Institute Of technology, Perur Chettipalayam, Pachapalayam, Coimbatore.

2 Under Graduate Student, Department of Computer Science & Engineering, Sri Ramakrishna Institute Of technology, Perur Chettipalayam, Pachapalayam, Coimbatore,

3 Under Graduate Student, Department of Computer Science & Engineering, Sri Ramakrishna Institute Of technology, Perur Chettipalayam, Pachapalayam,Coimbatore.

4 Under Graduate Student, Department of Computer Science & Engineering, Sri Ramakrishna Institute Of technology, Perur Chettipalayam, Pachapalayam, Coimbatore.

ABSTRACT

Since several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption, and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results.

1. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military, and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine, and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms.

2. Reversible Data Hiding

Reversible Data Hiding in Encrypted Domain (RDH-ED) [10] is a technology that studies reversible embedding of secret information using encrypted data as the carrier. This technology can not only protect plaintext data by encryption but also realize application expansion of ciphertext data by using secret information embedded in ciphertext, which plays an important role. Taking encrypted images as an example, using RDH-ED, users with authority can not only ensure the accurate extraction of secret information but also ensure the original data recovery without distortion after extraction and decryption.

3. Reversible Data Hiding Based on Error-Correction Redundancy

McEliece encryption introduces random errors during the construction process to establish NP-difficult linear decoding problem to achieve information protection. For data encrypted with the same pair of public and private keys, the introduced random error can produce a large amount of ciphertext redundancy. At the same time, the receiver can eliminate the redundancy with the verification operation of GOPPA code to ensure the accurate recovery.

4. Problem Statement

Arnold Transform is used in addition to chaotic encryption to add double layer security to data proposed scheme is robust to most of the image processing operations like JPEG compression, sharpening, cropping, median filtering, etc. the proposed scheme performs better in terms of robustness, security and imperceptivity. In Reversible Data Hiding in Images, textual data is embedded in images with acceptable loss in Image quality. During the data recovery process, the image should be restored to its original quality. In the proposed work, reversible data hiding is attempted either in encrypted images or in images with identified object that has to be spared from data hiding process.

5. Proposed System

Arnold Transform is used in addition to chaotic encryption to add double layer security to data proposed scheme is robust to most of the image processing operations like JPEG compression, sharpening, cropping, median filtering, etc. the proposed scheme performs better in terms of robustness, security and imperceptivity. In Reversible Data Hiding in Images, textual data is embedded in images with acceptable loss in Image quality. During the data recovery process, the image should be restored to its original quality. In the proposed work, reversible data hiding is attempted either in encrypted images or in images with identified object that has to be spared from data hiding process.

6. Methodology

6.1. CHAOS AND ARNOLD ENCRYPTION

A chaotic based encryption algorithm is an effective method for data encryption. Chaos signals possess the qualities of pseudo-randomness, irreversibility and dynamic behaviour. The systems having chaotic nature possess high sensitivity to initial parameters. The output chaotic sequence is similar to white noise having random behaviour with improved.

The Arnold transformation is mathematically represented as

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N)$$

The result of Arnold transform is an encrypted image which has a one-to-one correspondence with the original image. The pseudo-random nature of the Arnold encryption results in a scrambled image which is not possible to be cracked down without knowing the sequence used.

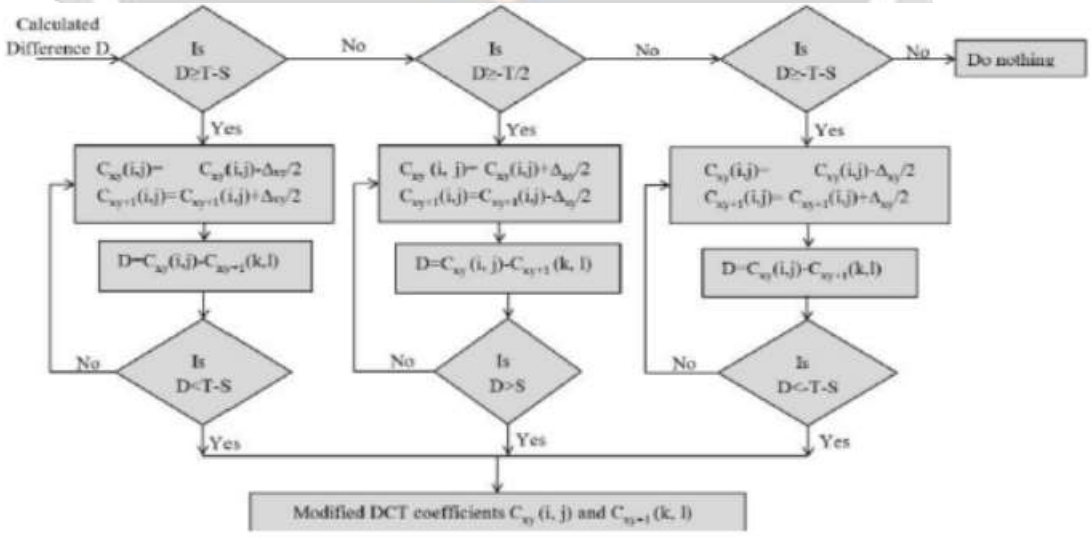
$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod} N)$$

6.2. WATERMARK AND COVER GENERATION

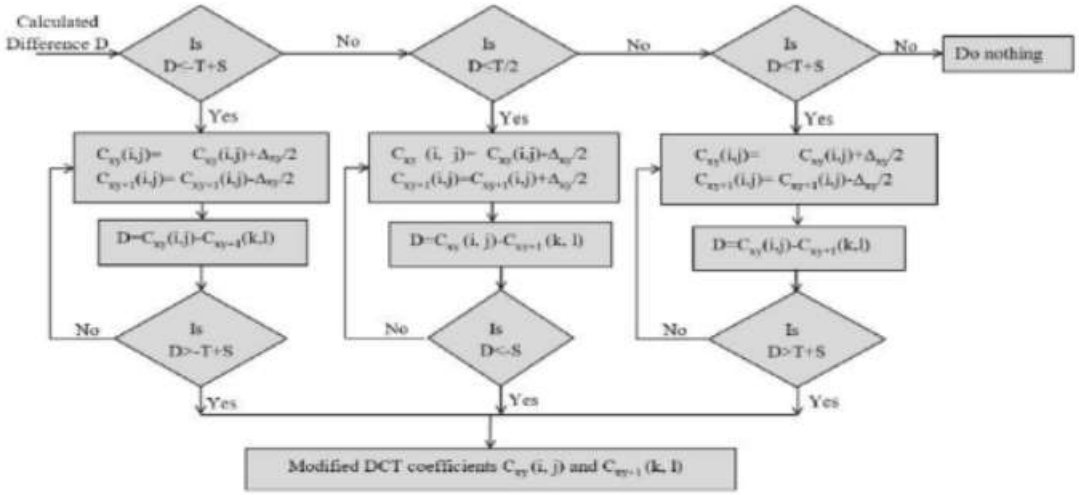
The input image 'I' is passed through the pre-processing unit which acts as a buffer for grayscale images and as a converter for color images. To carry out watermark embedding into the luminance part of the image the pre-processing unit converts the input RGB image into YCbCr image, where Y stands for luminance information, Cb stands for chrominance blue information and Cr stand for chrominance red information of the image. The luminance part 'Y' is put forward as cover for the watermark because modification of this part of the image brings less noticeable changes to actual image compared to the chrominance information. the regions defined above axis are for bit '1,' while the regions defined below the axis are for bit '0'. The modification factor is calculated as

$$\Delta_{xy} = \alpha \times \frac{DC(C_{xy}) - Median(C_{xy})}{DC(C_{xy})}$$

Secondly, the Arnold transform is performed on the sequence 'we1' to get the second level encrypted watermark 'we'. The input and encrypted watermarks are presented in Figure 4. The principle advantage of these two encryption methods is that we do not need a large overhead of keys. The number of iterations, initial value, and the logistic mapping parameter are the only keys that have to be used at the receiver to decrypt the encrypted data.



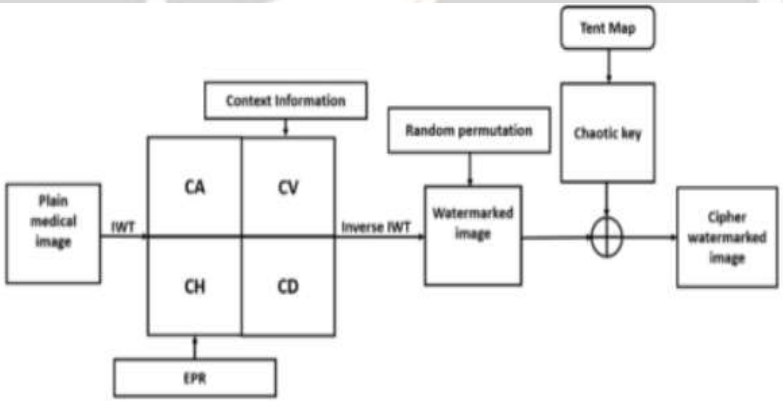
Flow Chart of Embedding 'bit 0'



Flow Chart for Embedding 'bit 1'

6.3. WATERMARK EMBEDDING

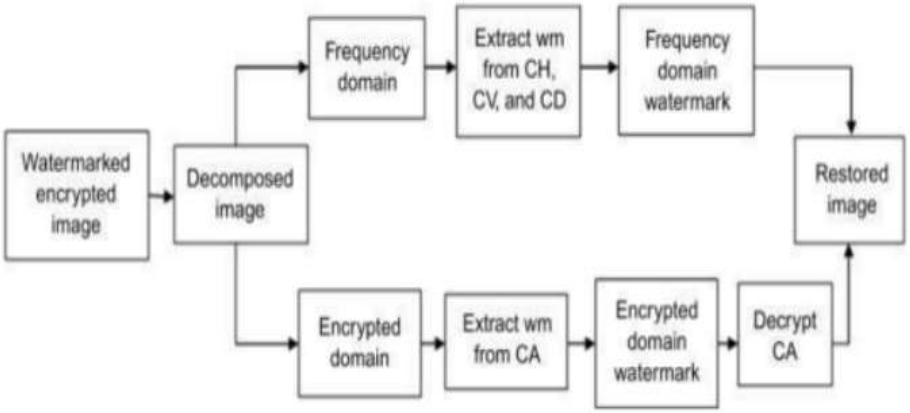
The pre-embedding difference between two coefficients. If 'D' lies in zone 1 or 3 then the coefficients Cxy (i, j) andCxy+1(k, l) aremodified in such a way that the difference between them reaches to zone 2, which is the nearest zone. the robustness of the proposed watermarking system. This guard band brings extra robustness to our watermark, which has been discussed in the extraction part. After complete embedding, inverse DCT (IDCT) of each modified DCT blocks is computed as shown in Figure 1. IDCT is followed by post processing operations, which include addition of 128 to each element of the modified Blocks B*x so that the pixel intensities ranging from 0 to 255.



Block diagram of watermark embedding and image encryption

6.4. WATERMARK EXTRACTION

Watermark extraction involves steps like pre-processing, the partition of the watermarked image into 16×16 blocks and 8×8 blocks; Only those DCT coefficients which are modified during embedding are used for watermark extraction. A watermark bit is obtained by analysing the difference between the two predefined coefficients. If the difference lies anywhere in zone 2 or zone 5, bit '1' is obtained while bit '0' is obtained if the difference lies either in zone 1 or zone 4. As already discussed, that between the information carrying zones there exists a guard band of 2S which is separating them from each other;



Block diagram for watermark extraction

7. Conclusion

This approach results in good performance on data hiding And it is very much safe, simple and faster. The future work of this paper will be minimizing the previous execution time and to deliver the better result in PSNR value with highest security, and also by including Watermarking technique it achieves high security in data transmission. Watermarking is the concept of copyright protection or digital ownership that can read by only authenticated person.

8. Reference

[1] H. Tao, L. Chongmin, J. M, Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," Journal of Applied Research and Technology., vol.12, no. 1, pp. 122–138, Feb. 2014.

[2] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," IEEE communications Magazine., vol. 39, no. 8, pp. 118-126, Aug. 2001.

[3] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks," EURASIP Journal on Advances in Signal Processing., pp. 1-22, Aug. 2014.

[4] N. Zivic., "Watermarking for Image Authentication," in Robust Image Authentication in the Presence of Noise, ist ed. Switzerland, Springer International Publishing, 2015, pp. 43-47 [Online].

[5] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," Journal of Biomedical Informatics, to be published. DOI

[6] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Reversible and high capacity data hiding technique for E-healthcare applications," Multimed Tools Appl., vol. 76, no.3, pp. 3943-3975, Feb. 2017.

[7] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, and G. M. Bhat, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection," Multimed Tools Appl., to be published. DOI: 10.1007/s11042-016-4253-x.

[8] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Information Hiding in Medical Images: A Robust Medical Image Watermarking System for E-Healthcare" Multimed Tools Appl., vol. 76, no. 8, pp. 10599–10633, Apr. 2017.

[9] R. Eswaraiah, and E. S. Reddy, "Robust medical image watermarking technique 17 for accurate detection of tampers inside region of interest and recovering original region of interest," IET Image Processing, vol. 9, no. 8, pp. 615-625, Jul. 2015.

[10] M. Benyoussef, S. Mabtoul, M. E. Marraki, and D. Aboutajdine, "Robust ROI Watermarking Scheme Based on Visual Cryptography: Application on Mammograms," Journal of Information Processing Systems, vol. 11, no. 4, pp. 495-508, Dec. 2015.

[11] L. Gao, T. Gao, G. Sheng, S. Zhang, "Robust medical image watermarking scheme with rotation correction," in Intelligent Data analysis and its Applications, Switzerland, Springer International Publishing, 2015, pp. 283-292.

[12] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," Multimedia Tools and Applications, vol. 76, no. 18, pp. 18985–19004, 2017

[13] A. Kanso, and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," Commun. Nonlinear Sci. Numer. Simulat., vol. 24, no. 1-3, pp. 98-116, Jan. 2015.