Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 2, July-2017, ISSN 2230-7540

Identification of Digital Image Using Protein Folding and Unfolding Structure

Vinay Kumar Pandey[1]* Manish Madhav Tripathi[2] Sonali Yadav[3]

[1]Department of Computer Science & Engineering, Integral University, Lucknow

[2]Department of Computer Science & Engineering, Integral University, Lucknow

[3]Department of Computer Science & Engineering, Integral University, Lucknow

Abstract – The past decade has witnessed an explosion-like storm of digitization in the life of many and its impact has its own reasons and consequences in other matters. Internet-connection able PCs have enabled the mobility of information and made convenient the carriage of digitized property closer to home than ever before. With the growing use and need of digital multimedia technology the security of multimedia information like audio, video, text and image have become a major concern. Integrity of image information is important especially when this type of data is used for authentication purpose e.g. medical diagnosis or court evidence. This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital information protection schemes. Many approaches are possible to protect visual data, digital watermarking is probably the one that has received most interest. The idea of fragile watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as intentional or unintentional alteration in extensive content of the digital image. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary. To cover the same objective this work propose an efficient image authentication and recovery approach using block wise fragile watermarking.

Keywords: Generic Fragile watermarking, Protein Folding and Unfolding

----------X----------

1. INTRODUCTION

The manner in which proteins, chains of amino acid residues, acquire their three-dimensional conformation has long been a subject of inquiry and many different explanations of the underlying mechanism have been proposed is the practice of imperceptibly altering a work to embed a message about that work. This technique contains two high level elements *Embedder* and *Detector* as shown in figure 1. The embedder takes two inputs. One is the payload we want to embed (e.g. either the watermark or secret message), other is the cover work in which we want to embed the payload. The output of embedder is presented as an input to the detector.

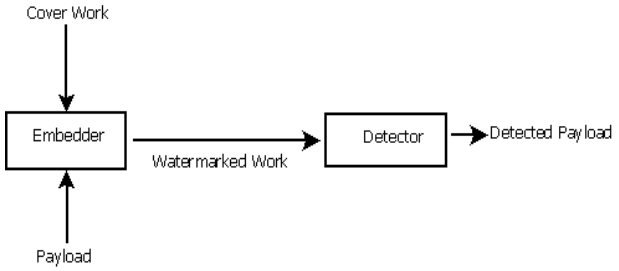

Figure 1: A generic watermarking system

Now a day's watermarking is used in various fields to provide security. Some watermarking applications are

- **Broadcast monitoring:** Identifying when and where works are broadcast by recognizing watermarks embedded in them.
- **Owner Identification:** Embedding the identity of the copy right owner as a water-mark.

- **Transaction tracking** Using watermark to identify people who obtain content legally but illegally redistribute it.

- **Content Authentication:** Embedding signature information in content that can be later checked to verify it has not been tampered.

- **Copy Control:** Using watermark to tell recording equipment what content may not be recorded.

- **Device Control:** Using watermark to make devices, such as toys react to displayed content.

- **Legacy Enhancement:** Using the watermark to improve the functionality of existing system. Watermarks are broadly classified into three categories viz. fragile, semi fragile and robust watermark.

1. **Fragile watermark:** A watermark that becomes undetectable after even minor modification of the work in which it is embedded.

2. **Robust watermark:** A watermark designed to survive on legitimate and everyday usage of content.

3. **Semi fragile watermarking:** A watermark that is unaffected by legitimate distortion but destroyed by illegitimate distortion.

II. PROPOSED APPROACH

Proposed algorithm [9] [10] [11] is bifurcated in to two major proposals. First proposal is Pixel-wise generic fragile watermarking scheme based on ARA bits using protein folding which is only used for alteration detection whereas second proposal is based on block-wise fragile watermarking using protein unfolding which detects the altered block as well as recover altered region with good approximation without changing the domain. First Proposal: Pixel-wise fragile watermarking based on ARA bits proposed algorithm is shown in figure 4 is based on ARA bits where ARA stands for Authentication, Relational and Associative bits.

- Code of the CUT and classifies each statement (i.e., determining its type).

- Determines whole information about the constructor, method signature.

- Now, all the method of the given source file stored in an array.

Watermark Embedding Procedure

Consider a gray scale host image I, having dimension $m \times n$. Then N represents the number of pixels, N= $m \times n$. So the gray scale value at each pixel of the image is denoted

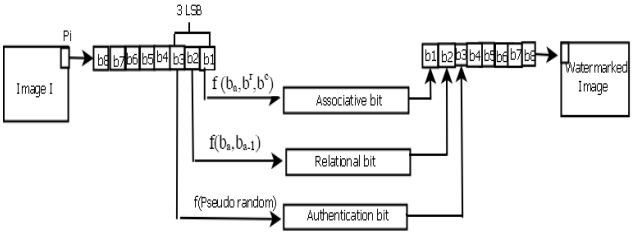

Figure 4: Block diagram of our first proposed approach

Step 1: For a given tampered image IT we generate a pseudo-random binary matrix having dimension m_n (same size as IT) with the same secret key which was used for embedding.

Step 2: For each pixel of IT , calculate the Associative bit then extract first LSB of all pixel of image IT . Compare the Associative bit with the extracted first LSB of corresponding pixel of IT . If there is mismatch, we mark those pixels as altered one.

Step 3: This step is carried out for those pixels which has qualified first Associative bit test i.e. Associative bit and first LSB is matched. Calculate the relational bit by using equation and then extract the second LSB of remaining unmarked pixels. Compare it with the Relational bit. If there is mismatch then those pixels will be marked as altered pixel.

Step 4: This last step is carried out for those pixels which have passed the relational bit test i.e. if no mismatch detected. From the pseudo random binary matrix we extract the binary value from the position corresponding to row and column of remaining unmarked pixels of IT We now compare the extracted binary value from pseudo random matrix and third LSB from IT . If there is mismatch, then those pixels will be marked as altered. If there will be no mismatch it means those pixels were not altered during any attack or gray scale value of altered pixel and original pixel is same.

III. EXPERIMENTAL RESULT & DISCUSSION

Since we have proposed two approaches based on pixel and block wise fragile watermarking scheme hence we will discuss experimental results and comparison separately for each technique

Experimental Results for Pixel wise Fragile Watermarking Scheme

Now, we demonstrate the effectiveness and accuracy of the proposed approach with experimental results and discuss the performance of our algorithm. The

simulation has been implemented in Matlab 2010 environment. We have taken many gray level test images as a host image with size 256_256 form a standard image database. First of all we do some major alteration in image which ensures the change in MSBs. Series (c) of all figure having black region shows the unaltered pixel whereas white region shows altered one.

Some altered pixels are undetectable because the five MSBs of those replaced pixels coincide with the original MSBs, they are regarded as “Unhampered

(a) (b) (c)

i. Baboon

IV. CONCLUSION

This thesis proposes an image authentication and restoration approach using block-wise fragile watermarking which is based on k-medoids clustering technique. Many of the ap- proaches for image restoration, proposed earlier, were in frequency domain but suggested scheme is utterly in spatial domain. Experimental results and Table 5 show the efficiency of proposed scheme which is not only good enough to perceive the altered block with high accuracy but also able to restore those tampered blocks with good imperceptibility. K-medoids is a representative object based clustering technique which ensures that the gray level value which is used to replace other gray value within a block, belongs to the same block. Hence we take the benefit of this property of k-medoids. Clustering for each block is done by using a common characteristic hence for each element within a single cluster has same characteristics.

V. REFERENCES

Anthony T. S. Ho, Xunzhan Zhu, Jun Shen, and Pina Marziliano (2008). Fragile Water- marking Based on Encoding of the Zeros of the - Transform *IEEE Transactions On Information Forensic and Security*, VOL. 3, NO. 3, September 2008.

Eugene T. Lin and Edward J. Delp. A review of fragile watermarking. *Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086*.

Hongjie He, Jiashu Zhang, Fan Chen (2007). Block-wise Fragile Watermarking Scheme Based on Scramble Encryption. *IEEE* 978-1-4244-4105-1/07.

Jiri Fridrich and Miroslav Goljan (1999). Images with Self-Correcting Capabilities. *IEEE*, 0-7803-5467-2/99.

Mi-Ae Kim and Won-Hyung Lee (2004). A Content-Based Fragile Watermarking Scheme for Image Authentication *Springer-Verlag Berlin Heidelberg*, AWCC 2004, LNCS 3309, pp. 258-265.

Corresponding Author

Vinay Kumar Pandey*

Department of Computer Science & Engineering, Integral University, Lucknow

E-Mail – vinaykprag85@gmail.com