International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 8 (April 2013), PP. 19-21

Enhanced Robust Watermarking Algorithm for various Applications

A.Dharmarajan[1], A.Hariram[2],
Assistant Professor,ANJAC, Sivakasi

Abstract:- This paper proposes the data embedding system for binary images including jpg, bmp, tiff, png. Shuffling is applied to the binary images in the first phase of this research work, which means that binary image pixels are convoluted into number of rows and columns. Next phase to shuffled binary images are interchanged and reconstructed in the form of original image. The water marked image was ready to send and receive through internet and mobile communication for various applications like medical, commercial and business applications. Our proposed algorithm maintains the complexity of execution is neutral than other methodology

Keywords:- Watermarking, Authentication, binary image, Shuffling, Reconstruction.

I. INTRODUCTION

Today's rapid evolution of innovative technology and the progress of computer networks along with the development of the Internet bring many advantages in the creation and distribution of image content. But beneath the ability of easy copying, transmitting and editing digital images the need for image content Permission to make digital or hard copies of all or part of this work for medical applications use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Digital images can be modified or forged by a wide variety of available manipulation software. The burden of proof of authenticity always lies with the person seeking to admit. He must provide other evidence to support this authenticity. Further, military photographs may determine target locations based on their content and interpretation. Thus, it is important to maintain the integrity of all images from capture to final use.

To prevent illegitimate tampering and fraudulent use of modified images authentication techniques were introduced. As known from the classical cryptography, to verify the exact data integrity, a signature may be generated from the source signal by the use of secure hash functions and encryption. A recipient decrypts the signature and matches it with the hash generated from the received signal. If even one bit of the signal has been modified, it will no longer match the signature, so any tampering can be detected. But this so-called fragile property is sometimes not practical when considering distribution of images. For instance, loss compression has to be performed to reduce the amount of data or signal processing is applied to correct gamma, to de-noise or to resample an image. These manipulations change the pixel values but not the content and hence not the authenticity. To tolerate certain kinds of signal processing semi-fragile authentication methods for digital images have been developed.

The aims to allow admissible manipulations such as JPEG compression, but to reject malicious manipulations that change the visual content. Commonly used techniques extract features representing the image content and re-embed these features as watermark information into the host image data .Some approaches involve image positions of edges, contours or zero-crossings in the spatial domain whose existence is proved during the verification process. Other methods are based on single coefficients or on relationships between pairs of different coefficients in the transform domain (e.g., DCT, DWT or DFT). The advantage of directly embedding authentication data as a watermark is, that the signature cannot get lost during format conversion operations. No additional data has to be submitted besides the watermarked image except some watermarking parameters and the key used for decryption. But, every single watermark bit that has to be embedded into the host data slightly modifies the image and degrades the visual quality. Hence, the right choice of the feature extraction as well as watermark embedding approach is decisive for a practical authentication system.

II. AUTHENTICATION FOR INPUT

The Computational Efficiency should be a major design criterion for an image authentication algorithm [1] [2], since the target device for implementation will be, e.g., a digital camera, mobile phone or Pocket PC with integrated camera with internet. But the security of the overall framework has to be explicitly considered as well. Many authentication frameworks lay to much emphasis on robustness, which brings into question security

issues for authentication applications. Often, the image content is pretended to be secured by protecting only the correct existence of mean values of extensive pixel areas. An attack, intended to change the image content, can maliciously operate on these local pixel areas as long as the mean values are not changed. For example, a forger is able to insert edges without raising an alarm when the authenticity is verified as long as he maintains the mean values of these extensive pixel areas. Our proposed system works efficiently in computations and comparisons during the shuffling process is takes average execution but and produces high level of features [3] [4] [5].

A) DECOMPOSING

The input image is converted to gray scale image and finds the R, G, B value. It is broken in to minimum number of segments by using the threshold value. These segmented image pixel values are shuffled using the following algorithm.

III. ALGORITHMS

This Water marking Algorithm for binary images of Various Fields to apply on the basis as follows:

A) Phase I: Shuffling

Step 1: Input from Decomposing unit.
Step 2: Setup the initial pixel value
Step 3: Continue the Shuffle task
Step 4: In Shuffling Pixels are rotated 'n' number of times.
Step 5: Iterations ended until the interchange of last column of the image matrix

In shuffling, the images are broken into several pieces and shuffled the pixel values as random [6]. Then, they are reconstructed by the following algorithm

B) *Phase II: Reconstruction*

Step 1: Construct the matrix for shuffled image.
Step 2: Put rank for the shuffled area.
Step 3: Construct the matrix according to the rank.

In reconstruction phase, the shuffled pixel values are ranked. They are rearranged by their rank. According to the rank value of the pixel, it can be retrieved by the user.

Fig 1) Diagram for Authentication of water marking system

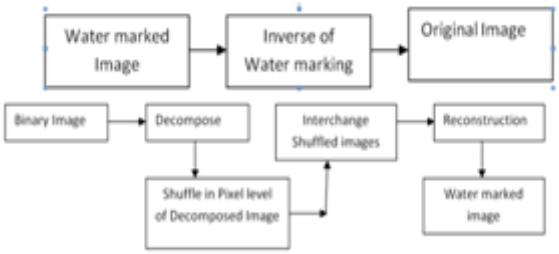

Fig 2) Diagram for Extracting the water marking image

Fig 3) Input image

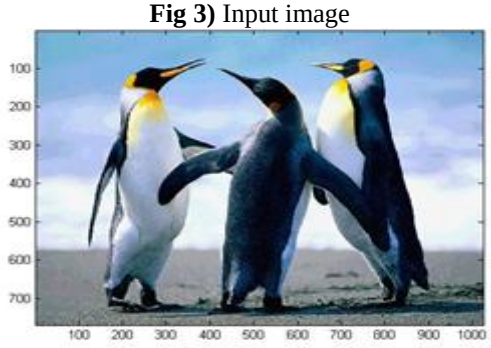

fig 4) watermarked image

Fig. 5) Shifted watermarked Image
Fig.6) Reconstructed Watermark image

IV. CONCLUSION

This system embedding a shifted value into the image, so that changes to the resultant images can be identified with high probability with minimum time constraints. Shuffling is applied before embedding to equalize uneven embedding capacity. The algorithm can be applied to detect unauthorized use of access in binary image format, to detect alteration on images. It is convenient to apply in more research and application developments, such as medical, business Commercial purposes.

REFERENCES

[1]. P. S. L. M. Barreto, H. Y. Kim and V. Rijmen,"Toward a Secure Public-Key Block wise Fragile Authentication Watermarking," IEE Proc. Vision, Image and Signal Processing, vol. 149, no. 2, pp. 57-62, 2002.

[2]. C. T. Li, D. C. Lou and T. H. Chen, "Image Authentication and Integrity Verification via Content Based Watermarks and a Public Key Cryptosystem," IEEE Int. Conf. Image Processing, 2000, vol.3,

[3]. G.Pass, Y.J.Wu and Z..A Novel Data Hiding Method for Two – color Images " , Lecture Notes in Computer Science Information and Communications Security, Springer-Verlag, NOV. 2001, PP. 261 – 270.

[4]. M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary image,"IEEE Int.Conf. Multimedia

[5]. Wen-Yuan Chen and Chen-Chung Liu, " Robust watermarking & Expo (ICME'00), NewYork,2000 scheme for binary images using large-cluster algorithm with a Hamming Code", Optical Engineering,Vol. 45, Iss.1, 2006.

[6]. Jeanne chan, Tung-shan chen, " A New Data Hiding Method in Binary Image" , Proc. IEEE Fifth International Symposium on Multimedia Software Engineering (ISMSE ' 03). 2003.