WATERMARKING FRAMEWORK FOR AUTHENTICATION AND SELF-RECOVERY OF TAMPERED COLOUR IMAGES

M. Mariya Asha Rani
1PG schola , Department of Electronics Communication Engineering
St.Michael College of Engineering and Technology, Tamilnadu, India

V. Kumaresan
Assistant Professor, Department of Electronics Communication Engineering
St.Michael College of Engineering and Technology, Tamilnadu, India

Abstract

Due to the advances in computer-based communication and health services over the past decade, the need for image security becomes urgent to address the requirements of both safety and non-safety in all applications. Methods of authentication and self-recovery of tampered information in digital images have been in constant development during the last years. The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and LU is applied to figure out the transformation in the original image. Then generates the authentication watermarks, which are based on XOR operations on non-overlapping blocks, subsequently by using a half toning technique the recovery watermark is generated. The proposed half toning technique coded in lower complexity and low power image processing capability of proposed framework. To evaluate the quality of the obtained images, the objective criterion of peak signal-to-noise ratio (PSNR) and Tampering ratio are used. The experimental results demonstrate the effectiveness of our method in comparisons with other schemes reported in the literature, where the quality of the watermark images, the quality of the reconstruction images and the recovery rate of each scheme were evaluated

Introduction

The widespread emergence of computer networks and the popularity of electronic managing of medical records have made it possible for digital medical images to be shared across the world for services such as telemedicine, tele radiology, tele diagnosis, and teleconsultation. Instant diagnosis and understanding of a certain disease as well as cutting down the number of misdiagnosis has had extensive social and economic impact, clearly showing the need for efficient patient information sharing between specialists of different hospitals. In the handling of medical images, the main priority is to secure protection for the patient's documents against any act of tampering by unauthorized persons. Thus, the main concern of the existing electronic medical system is to develop some standard solution to preserve the authenticity and integrity of the content of medical images.

Basic Concepts in Watermarking Scheme

The watermarking concept is closely related to two other fields: cryptography and steganography. These areas fall under the domain called data security system. Cryptography is a method for sending a message in a secure format that only the authorized person can decode and read. This is known as a "secret writing."

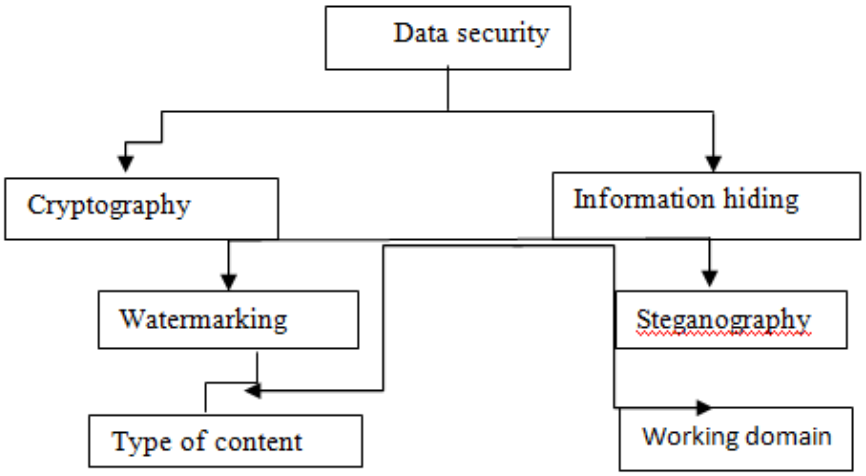

Figure 1 Security system and different classification of watermarking

Water Marking System

Digital watermarking is the procedure of embedding information (i.e., a watermark) into the host object in such a way that the watermark image/data can be detected by authorized individuals, for assertion of authenticity purposes. The host signal can be a video, audio, image, 3D mesh, etc., while the watermark can be a logo, image, serial number, owner's ID, name, or any other information which shows ownership of the host signal. These signatures are normally converted into a binary sequence before being embedding into the host signal.

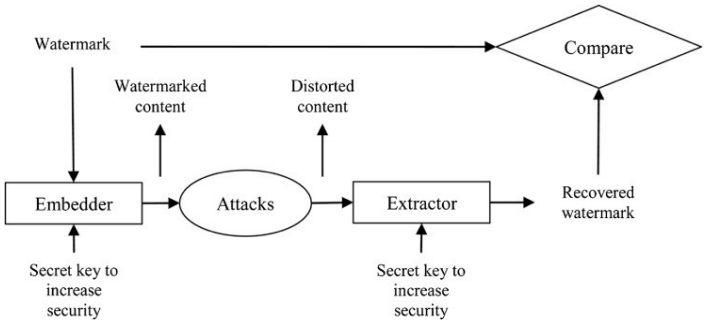

Figure 2 Typical water marking system framework

Existing System

In existing system, a fragile watermarking based scheme for image authentication and self-recovery for medical applications. This scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block wise SVD into the least significant bit (LSB) of the image In existing system ,a fragile watermarking based scheme for image authentication and self-recovery for medical applications. This scheme locates image tampering as well as recovers the original

image. A host image is broken into 4×4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block wise SVD into the least significant bit (LSB) of the image pixels to figure out the rmation in the original image.

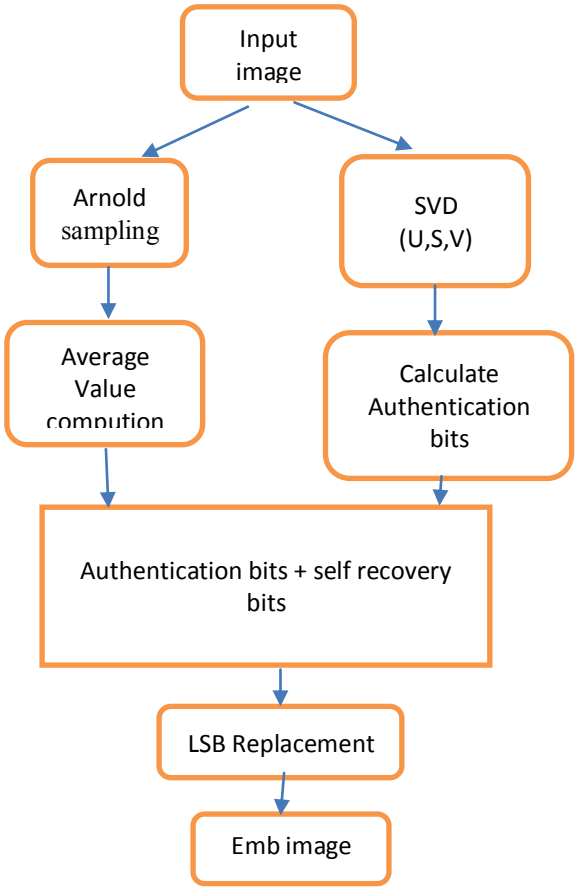

Figure 3 Block representation of watermark embedding method

The host image is divided into small blocks of size 4×4 and the LSB of all these blocks are set as zero .This division guides us to calculate the tamper localization information for each block separately by the help of SVD operation on each 4×4 blocks. After SVD is computed for each block, the corresponding traces

Singular Vector Decomposition

Singular value decomposition is a method of decomposing a matrix into three other matrices:

$$A = USV^T$$

where,

- A is an $m \times n$ matrix
- U is an $m \times n$ *orthogonal* matrix
- S is an $n \times n$ *diagonal matrix*
- V is an $n \times n$ orthogonal matrix

where, I is the *identity matrix*. Using the orthogonality property, we can rearrange (1) into the following pair of eigenvalue equations:

$$AA^TU = US^2$$

$$A^TAV = VS^2$$

Proposed System

This work proposes a new LU decomposed half toning scheme for image authentication and self-recovery for medical applications. The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and LU is applied to figure out the transformation in the original image. Then generates the authentication watermarks, which are based on XOR operations on non-overlapping blocks, subsequently by using ahaif toing

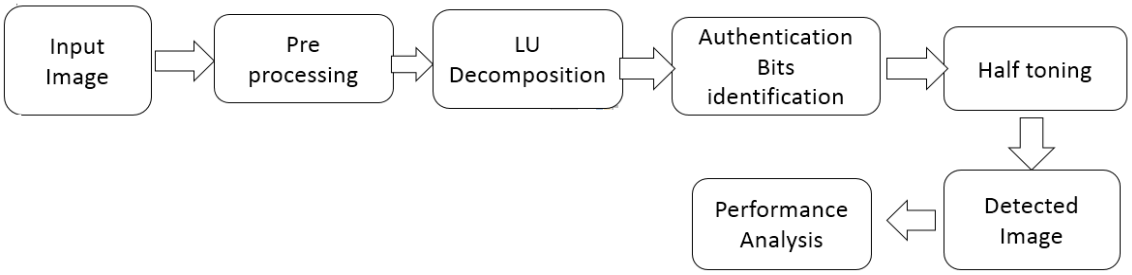

Figure 4 Proposed architecture

The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and LU decomposition is applied by inserting the traces of block wise LU decomposition into the least significant bit (LSB) of the image pixels to figure out the transformation in the original image.

If an image is stored as a JPEG-image on your disc we first read it into Mat lab. However, in order to start working with an image, for example perform a wavelet transform on the image, we must convert it into a different format.

Intensity Image (Gray Scale Image)

This is the equivalent to a "gray scale image" and this is the image we will mostly work with in this course. It represents an image as a matrix where every element has a value corresponding to how bright/dark the pixel at the corresponding position should be colored. There are two ways to represent the number that represents the brightness of the pixel: The double class (or data type). This

assigns a floating number between 0 and 1 to each pixel. The value 0 corresponds to black and the value 1 corresponds to white.

Binary Image

This image format also stores an image as a matrix but can only color a pixel black or white. It assigns a 0 for black and a 1 for white. \

Results & Discussion

Screenshots

Figure 5 Input image

Above figure 5 shows input image for our embedding process. In this stage image converted into gray scale image and resized to required stage

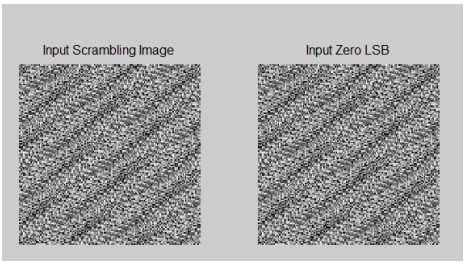

Figure 6 Scrambled and LSB numbered image

Above Figure 6 shows scrambled image and LSB renumbered image for our embedding process. In this stage image authentication bits are identified using Arnold sampling

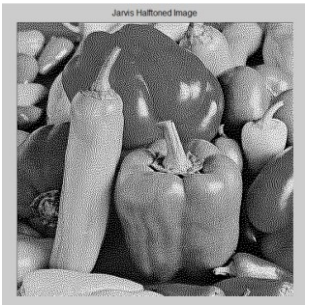

Figure 7 Half toning image

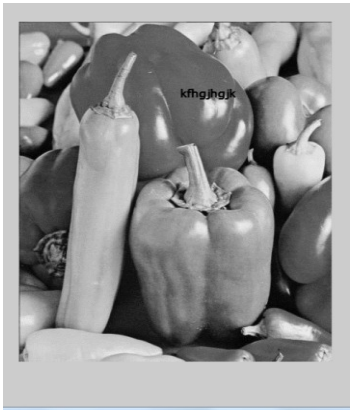

Figure 8 Received image

Above figure 8 shows received image after performing tampering

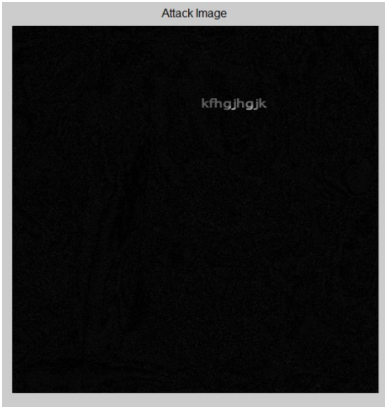

Figure 9 Tamper detected image

Above figure 9 shows tamper identified image using our authentication bits

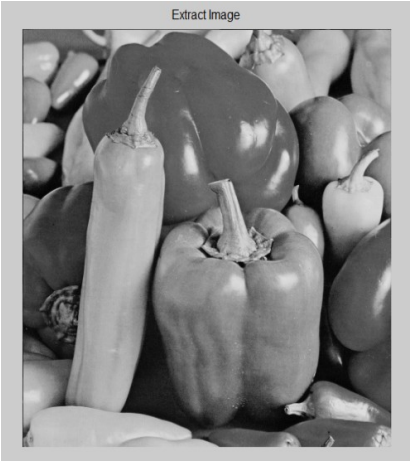

Figure 10 Recovered image

Above figure 10 shows recovered image by performing LSB zero and LU decomposition

Performance Evaluation

Below table shows improved SNR calculation before and after embedding and extraction

Table 1 Improved SNR calculation before and after embedding and extraction

S . No	Image set	PSNR
1	1	50.2302
2	2	51.0662
3	3	51.1394
4	4	50.7783

Conclusion

Watermarking is a crucial technique in the copy right identification mechanisms of digital assets. It is widely recognized as one of the key issues of data copyright protection in this work we considered the defect of traditional watermarking schemes, while dealing with the non numeric attributes. This project presents a LU and half toning based tamper detection scheme using grouped block method to offer more security and provide a supplementary way to locate the attacked areas inside different medical images. Two authentication bits namely block authentication and self-recovery bits were used to survive the vector quantization attack. The usage of authentication makes it possible to recover the tampered region from the neighboring blocks, which ultimately increases the NCC and PSNR of the recovered host. Presents a LU and half toning based tamper detection scheme using grouped block method to offer more security and provide a supplementary way to locate the attacked areas inside different medical images. Two authentication bits namely block authentication and self-recovery bits were used to survive the vector quantization attack. The usage of authentication makes it possible to recover the tampered region from the neighboring blocks, which ultimately increases the NCC and PSNR

References

1. Uhammad Sajjad, Khan Muhammad, Sung Wook Baik, Seungmin Rho, Zahoor Jan, Sang-Soo Yeo,Irfan Mehmood, Mobile-cloud assisted framework for
2. selective encryption of medical images with steganography for resource-constrained devices ,Multimedia Tools and Applications, Volume 76, Issue3, pp 3519–3536, 2017
3. Hamza, R., Muhammad, K., Lv, Z., & Titouna, F.(2017). Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive
4. and Mobile Computing.(https://doi.org/10.1016/j.pmcj.2017.03.011)
5. R. Hamza, K. Muhammad, A. Nachiappan, and G. R.González, "Hash based Encryption for Key frames of Diagnostic Hysteroscopy," IEEE Access, vol. PP
6. 1-1, 2017.(https://doi.org/10.1109/ACCESS.2017.2762405)

7. Jan, Z., Khan, A., Sajjad, M. et al. A review on automated diagnosis of malaria parasite in microscopic blood smears images, Multimedia Tools and Applications, 2017: 1–26.https://doi.org/10.1007/s11042-017-4495-2
8. Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, Sung Wook Baik, Image steganography using uncorrelated color space and its application for security of visual contents in on line social networks, In Future Generation Computer Systems,2016. https://doi.org/10.1016/j.future.2016.11.029.
9. Yu-Chen Hu, Chun-Chi Lo, Chang-Mingwu, Wu-Lin Chen, And Chia-Hsien Wen .Probability-based tamper detection scheme for compressed images based on quantization levels modification. International Journal of Security and Its Applications, 7(3):11–32, 2013.
10. Shao-Hui Liu, Hong-Xun Yao, Wen Gao,And Yong-Liang Liu. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. Applied Mathematics and Computation,185(2):869–882, 2007.
11. Ninghui Li, Wenliang Du, And Danboneh. Oblivious signature-based envelope .Distributed Computing, 17(4):293–302, 2005
12. Toshihiko Matsuo And Kaorukurosawa. On parallel hash functions based on block-ciphers. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 87(1):67–74, 2004.
13. Shan Suthaharan. Fragile image water marking using a gradient image for improved localization and security. Pattern Recognition Letters, 25(16):1893–1903, 2004.