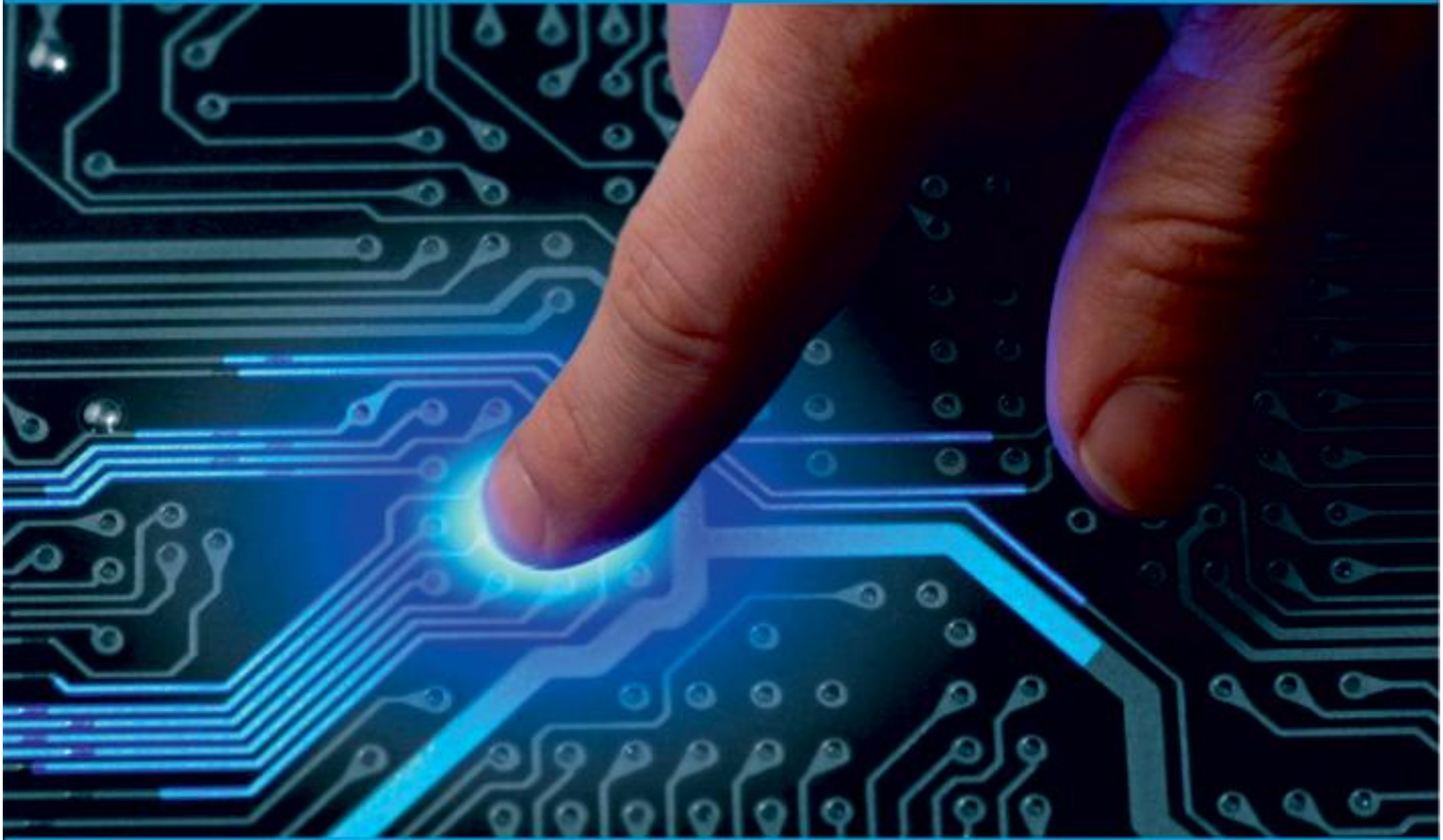
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Image Tampering Detection and Self Recovery Scheme Using SVD Based Authentication Bits

K.Gunasekaran[1], J.Kishore Kumar[2], H.Karthick[3], P.Kalanidhi[4]

Assistant Professor, Dept. of CSE, Panimalar Engineering College, Tamil Nadu, India[1]

UG Student, Dept. of CSE, Panimalar Engineering College, Tamil Nadu, India [2, 3, 4]

ABSTRACT: Copy-move forgery is one of the most commonly used manipulations for tampering digital images. Key point-based detection methods have been reported to be very effective in revealing copy-move evidences, due to their robustness against various attacks, such as large-scale geometric transformations. However, these methods fail to handle the cases when copy-move forgeries only involve small or smooth regions, where the number of key points is very limited. This project proposes a new fragile watermarking-based scheme for image authentication and self-recovery for image applications. The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and QR decomposition is applied by inserting the traces of block wise QR into the least significant bit (LSB) of the image pixels to figure out the transformation in the original image. Two authentication bits namely block authentication and self-recovery bits are used to survive the vector quantization attack. The insertion of self-recovery bits is determined with Arnold transformation, which recovers the original image even after a high tampering rate. QR-based watermarking information improves the image authentication and provides a way to detect different attacked area of the watermarked image. The proposed scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared to the state-of-the art methods, the proposed scheme greatly improves both tamper localization accuracy and the Peak Signal to Noise Ratio (PSNR) of self-recovered image.

KEYWORDS: watermarking-basedscheme,left significant bit,Arnold transformation

I.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 [16]. 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.

Accordingly, one solution for tackling the above issue is the use of digital watermarking. In other words, watermarking can enhance the security of medical images by inserting special information, called a watermark or hidden data, in a non-conspicuous way. Watermark information is usually inserted in a binary format to the pixel value of the host image [7][8]. This information can later be retrieved and checked whether the medical image is distributed with the actual source (authenticity) or belongs to the correct patient (integrity).

II.LITERATURE SURVEY

Nguyen et al proposed a method which limits the range of threshold values. Instead of brute-force searching all threshold values in HPS method or choosing threshold values unsystematically. This method classifies and chooses a number of thresholds whose frequencies satisfy the vital capacity to gain the best imperceptibility. In addition, the proposed method puts forward a secure way of watermark. The results of the experiment on natural images and medical images show the method meets the imperceptibility and high capacity.

Digital watermarking technique for digital medical images,2012

Wei Song et al presented a digital medical image contain more important information, and any change of it may result in physiotherapy accident. How to authenticate the digital images' reality and integrity become so important that we should use new technique to protect them. Digital watermarking is a technique that embeds important data into host multimedia, and it can be used in digital right management, authentication and data hiding. In this paper, author analyzed the character of medical images and watermarking technique. And give the basic procedure of them, and analyze the performance of these algorithms.

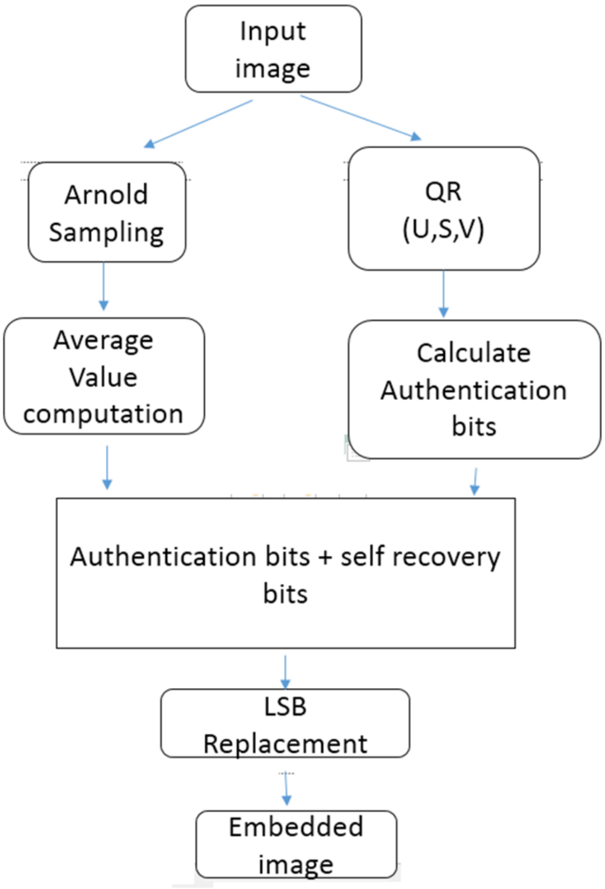
Benchmark for Medical Image Watermarking,2007

Medical images with EPR embedded in it can be used for transmission, storage or telemedicine applications. There is a need of specific standards for the evaluation of watermarking techniques used for embedding EPR data on medical images. No existing benchmark addresses this issue. There are no universally accepted performance measures applicable for every watermarking system. In this work a benchmark is proposed for the evaluation of medical image watermarking and data hiding techniques.

A Robust Double Watermarking Technique for Medical Images with Semi-Fragility,2017

Lendale et al presented an innovative authentication technique for medical images based on double watermarking technology. The proposed multi transform based watermarking technique utilizes Arnold Transform (AT), Discrete Wavelet Transform (DWT) and Discrete Cosine transform (DCT) leading to an enhanced robust double water marking technique with semi - fragility (RDWTSF) for medical images. The proposed methodology superimposes a spectral method (DCT) on a multi-resolution transform (DWT) while inserting the corresponding invisible watermarks onto the host image in two steps. Prior to these steps the host image is subjected to AT which reduces the spatial correlation among the pixels of the host image by disordering their location which retain many coefficients DCT and DWT making them suitable for computation and realizes high-quality, robustness and semi-fragility

III.PROPOSED SYSTEM


Input image
Arnold Sampling
QR (U,S,V)
Average Value computation
Calculate Authentication bits
Authentication bits + self recovery bits
LSB Replacement
Embedded image

The proposed 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 transformation in the original image. Two authentication bits namely block authentication and self-recovery bits are used to survive the vector quantization attack. The insertion of self-recovery bits is determined with Arnold transformation, which recovers the original image even after a high tampering rate. SVD-based watermarking information improves the image authentication and provides a way to detect different attacked area of the watermarked image

Square matrix

Any real square matrix A may be decomposed as

A=QR

where Q is an orthogonal matrix (its columns are orthogonal unit vectors meaning Q QT = QT Q = 1) and R is an upper triangular matrix (also called right triangular matrix). If A is invertible, then the factorization is unique if we require the diagonal elements of R to be positive.

If instead A is a complex square matrix, then there is a decomposition A = QR where Q is a unitary matrix (so Q Q* = Q* Q = 1)).

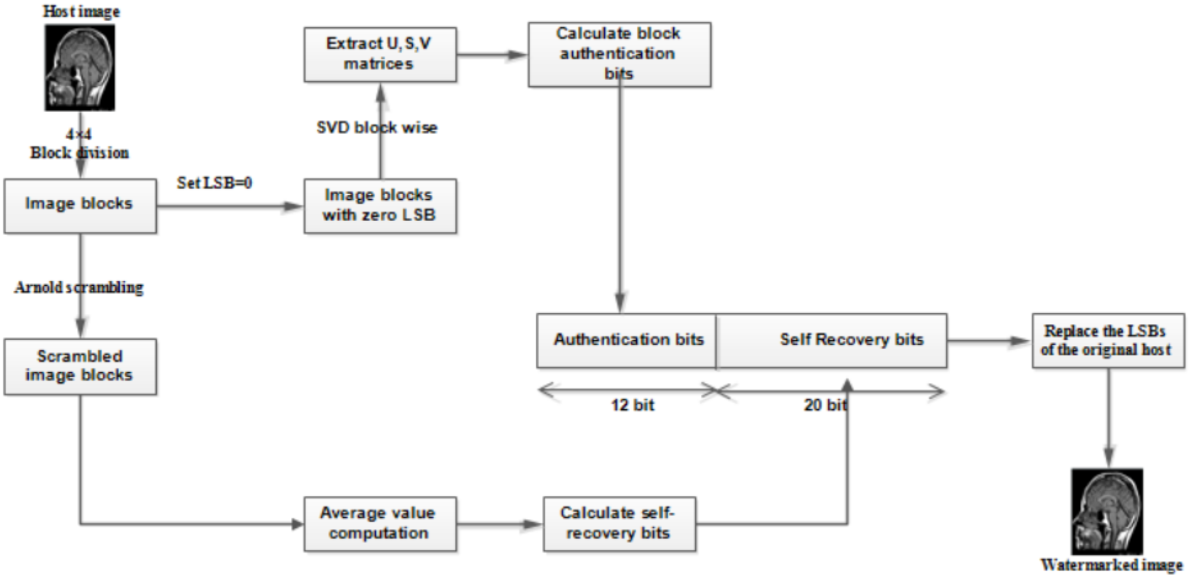
If A has n linearly independent columns, then the first n columns of Q form an orthonormal basis for the column space of A. More generally, the first k columns of Q form an orthonormal basis for the span of the first k columns of A for any $1 \leq k \leq n$.[1] The fact that any column k of A only depends on the first k columns of Q is responsible for the triangular form of R.

Rectangular matrix

More generally, we can factor a complex m×n matrix A, with $m \geq n$, as the product of an m×m unitary matrix Q and an m×n upper triangular matrix R. As the bottom (m−n) rows of an m×n upper triangular matrix consists entirely of zeroes, it is often useful to partition R, or both R and Q:

IV.EXISTING SYSTEM

AbdulazizShehab proposes a new 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 transformation in the original image. Two authentication bits namely block authentication and self-recovery bits are used to survive the vector quantization attack. The insertion of self-recovery bits is determined with Arnold transformation, which recovers the original image even after a high tampering rate. SVD-based watermarking information improves the image authentication and provides a way to detect different attacked area of the watermarked image. This scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared to the state-of-the art methods, this scheme greatly improves both tamper localization accuracy and the Peak signal to noise ratio (PSNR) of self-recovered image.

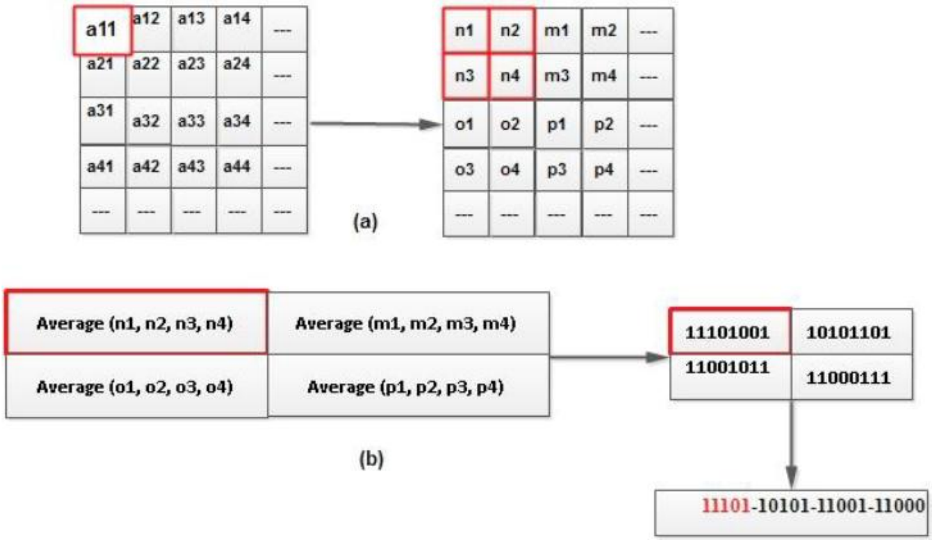


. The host image is divided into small blocks of size 4×4 and the LSB of all these blocks are set as zero. This division guides us to calculate the tamper localization information for each block separately by the help of SVD operation on each 4×4 blocks. After SVD is computed for each block, the corresponding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

The digital image can be seen as a two-dimensional matrix. When the size of the image is N, then I have N × N elements, the subscript x, y stands for the position of pixel, x, y ∈ {0, 1, 2..., N-1}. Let x, y corresponds to the x, y of Arnold scrambling, for each pair x, y, after all do Arnold Sampling, become x' and y', which equivalent to the original image of the point from (x, y) move to the = (x ', y'), so realized the movement of pixels in the image, the image with Arnold Sampling traverse all the points to complete a picture of Arnold scrambling.

Recovery in Arnold Sampling Algorithm:

Arnold Sampling recovery has two ways: one is the application of its periodicity, and the other is the pursuit of its inverse matrix to the inverse transformation. It is very natural to leverage the periodicity of Arnold scrambling method. By research of it before, we can come to this conclusion: For the digital image of N × N pixels, as long as meet non-1 positive integer N, The Arnold Sampling has periodicity. Extend to an arbitrary Scrambling time of n, you need to proceed (mN-n mod mN) times Arnold Sampling transformation. However, the times of scrambling are related to the order of N, in general, if N is the number of higher-order cases, the cycle is relatively long.



Singular Vector Decomposition

Today, singular value decomposition has spread through many branches of science, in particular psychology and sociology, climate and atmospheric science, and astronomy. It is also extremely useful in machine learning and in both descriptive and predictive statistics.

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

- A is an m × n matrix
- U is an m × n orthogonal matrix
- S is an n × n diagonal matrix
- V is an n × n orthogonal matrix

The reason why the last matrix is transposed will become clear later on in the exposition. Also, the term, “orthogonal,” will be defined (in case your algebra has become a little rusty) and the reason why the two outside matrices have this property made clear. For the moment, we will assume that m ≥ n. What happens when this isn’t true is quite interesting and is one of the keys, in my opinion, to understanding singular value decomposition.

This is already becoming quite complicated so I will rewrite Equation (1) using summation notation. This is my go-to method of proceeding whenever I am having trouble with a matrix equation. In this case, while it doesn’t make anything simpler, it does make everything absolutely explicit:Note how we’ve collapsed the diagonal matrix, S, into a vector, thus simplifying the expression into a single summation. The variables, $\{s_i\}$, are called singular values and are normally arranged from largest to smallest:The columns of U are called left singular vectors, while those of V are called right singular vectors.We know that U and V are orthogonal, that is:Where I is the identity matrix. Only the diagonals of the identity matrix are 1, with all other values being 0. Note that because U is not square, we cannot say that U Transpose(U)=I, so U is only orthogonal in one direction.Using the orthogonality property, we can rearrange

$$s_{i+1} \leq s_i$$

Numerical procedure

Since Transpose(A)A is the same size or smaller than A Transpose(A), a typical procedure is to plug Equation (3) into an eigenvalue calculator to find V and S²and then find U by projecting A onto V:

$$a_{ij} = \sum_{k=1}^{n} u_{ik} s_k v_{jk}$$

$$AA^T U = US^2$$

Note that the method is completely symmetric; U and V change places when Ais transposed:

Thus, if m < n, we can transpose A, perform the decomposition, then swap the roles of U and V.

In this case, U will be an m × m square matrix since there can be at most m non-zero singular values, while V will be an n × m matrix.

LSB replacement

The cover image used is a color image. Before embedding the data, we use 8-bit secret key and XOR with all the bytes of the message to be embedded. Message is recovered by XOR operation by the same key. Every pixel value in this image is analyzed and the following checking process is employed.

The Steps to be carried out for implementation of the technique is as follow.

1. If the value of the pixel say gi, is in the range 240 <=gi<=255 then we embed 4 bits of secret data into the 4 LSB's of the pixel. This can be done by observing the first 4 Most Significant Bits (MSB's). If they are all 1's then the remaining 4 LSB 's can be used for embedding data.

2. If the value of gi (First 3 MSB 's are all 1's), is in the range 224 <=gi<=239 then we embed 3 bits of secret data into the 3 LSB's of the pixel.

3. If the value of gi (First 2 MSB's are all 1's), is in the range 192 <=gi<=223 then we embed 2 bits of secret data into the 2 LSB's of the pixel.

4. And in all other cases for the values in the range 0 <=gi<=192 we embed 1 bit of secret data in to 1 LSB of the pixel.

Similarly, we can retrieve the secret data from the values of an image by again checking the first four MSB 's of the pixel value and retrieve the embedded data. These steps have been carried out to get efficient results.

V.CONCLUSION

In this work, we have proposed a fast and effective key point-based copy-move forgery detection and localization technique. This project presents a QR based fragile watermarking 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 Arnold transform makes it possible to recover the tampered region from the neighboring blocks, which ultimately increases the NCC and PSNR of the recovered host.

REFERENCES

[1] Muhammad Sajjad, Khan Muhammad, Sung WookBaik, Seungmin Rho, Zahoor Jan, Sang-Soo Yeo, IrfanMehmood, Mobile-cloud assisted framework for
selective encryption of medical images with steganography for resource-constrained devices, Multimedia Tools and Applications, Volume 76, Issue 3, pp 3519–3536, 2017

[2] Hamza, R., Muhammad, K., Lv, Z., &Titouna, F. (2017). Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive
and Mobile Computing. (https://doi.org/10.1016/j.pmcj.2017.03.011)

[3] R. Hamza, K. Muhammad, A. Nachiappan, and G. R. González, "Hash based Encryption for Keyframes of Diagnostic Hysteroscopy," IEEE Access, vol. PP
1-1, 2017. (https://doi.org/10.1109/ACCESS.2017.2762405)

[4] 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

[5] Khan Muhammad, Muhammad Sajjad, IrfanMehmood, Seungmin Rho, Sung WookBaik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, In Future Generation Computer Systems, 2016 https://doi.org/10.1016/j.future.2016.11.029.

[6]Yu-Chen Hu, Chun-Chi Lo, Chang-Ming Wu, Wu-Lin Chen, And Chia-Hsien Wen. Probability-Based Tamper Detection Scheme For Btc Compressed Images Based On Quantization Levels Modification. International Journal Of Security And Its Applications, 7(3):11–32, 2013.

[7] 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.

[8] Ninghui Li, Wenliang Du, And Dan Boneh. Oblivious Signature-Based Envelope. Distributed Computing, 17(4):293–302, 2005

[9] Toshihiko Matsuo And Kaoru Kurosawa. On Parallel Hash Functions Based On Block-Ciphers. Ieice Transactions On Fundamentals Of Electronics, Communications And Computer Sciences, 87(1):67–74, 2004.

[10] Shan Suthaharan. Fragile Image Watermarking Using A Gradient Image For Improved Localization And Security. Pattern Recognition Letters, 25(16):1893–
1903, 2004.

[11] Chun-Shien Lu And H-Ym Liao. Structural Digital Signature For Image Authentication: An Incidental Distortion Resistant Scheme. Multimedia, Ieee Transactions On, 5(2):161–173, 2003.

[12] Ping Wah Wong And Nasir Memon. Secret And Public Key Image Water- Marking Schemes For Image Authentication And Ownership Verification. Image Processing, Ieee Transactions On, 10(10):1593–1601, 2001.

[13] Matthew Holliman And Nasir Memon. Counterfeiting Attacks On Obliv- Ious Block-Wise Independent Invisible Watermarking Schemes. Image
Processing, Ieee Transactions On, 9(3):432–441, 2000.

[14] N Memon, S Shende, And Ping Wah Wong. On The Security Of The Yeung-Mintzer Authentication Watermark. In Is And Ts Pics Conference, Pages 301–306. Society For Imaging Science & Technology, 1999.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☐ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com