IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 20, Issue 1, Ser. 1 (Jan. – Feb. 2025), PP 54-61
www.iosrjournals.org

Secure Composition-Based Authentication For Image Forgery Detection

Geena Vidya S
M.E, Applied Electronics
Department Of Electronics And Communication
Sathyabama Institute Of Science And Technology, Chennai, India

Dr Annadevi E
Associate Professor, Department Of Electronics And Communication
Sathyabama Institute Of Science And Technology
Chennai, India

Dr R M Joany
Associate Professor, Department Of Electronics And Communication
Sathyabama Institute Of Science And Technology
Chennai, India

Abstract
In the era of digitalization, the integrity and authenticity of visual content face significant challenges due to the proliferation of image forgery. This paper presents a novel concept of authentication utilizing half-toning and QR code composition for robust forgery detection in images. The proposed method integrates two distinct techniques to enhance the security and reliability of authentication mechanisms. Firstly, half-toning is employed to convert the image into a binary representation, reducing its complexity while preserving essential features. Subsequently, QR codes are strategically composed within the image, encoding cryptographic information to verify its authenticity. This fusion of techniques not only ensures a high level of security but also facilitates efficient forgery detection through digital analysis. By embedding authentication data directly into the image, the proposed approach mitigates the risk of tampering and manipulation, thereby safeguarding against malicious activities. Experimental output demonstrate the effectiveness and resilience of the proposed method in accurately detecting and verifying image authenticity, thereby offering a promising solution to combat image forgery in diverse applications.

Date of Submission: 12-02-2025 Date of Acceptance: 22-02-2025

I. Introduction

The rise of computer networks & the adoption of electronic medical record management have enabled sharing digital medical images globally for telemedicine, tele radiology, tele diagnosis, & teleconsultation. Instant diagnosis & accurate disease understanding have had significant social & economic impacts, highlighting the importance of efficient patient information sharing among hospital specialists. Protecting patient documents from unauthorized tampering is a top priority in medical image management. The primary focus of electronic medical systems is to establish standard solutions to maintain the authenticity and integrity of medical image content.

One approach to address these concerns is through watermarking. Essentially, watermarking can bolster the security of medical images by embedding special information, known as a watermark or hidden data, discreetly. Usually, this information is inserted in binary form into the pixel value of the original image. This embedded information can subsequently be extracted and verified to confirm the authenticity of the source and ensure that it corresponds correctly to the patient's records.

Different views help classify watermarking methods[13]. Various categories of watermarking methods are explained below. Based on the concept of embedding, we can categorize watermarking algorithms as spatial or transform domain. In the spatial domain, watermark information is directly inserted into the pixel value of the host image. These methods are quick and straightforward, offering a high capacity for adding watermarks. While spatial domain methods have advantages like resistance to cropping attacks, they struggle with noise or lossy compression attacks. Moreover, third parties can easily modify embedded watermarks in this domain.

On the other hand, in the transform domain, watermarked images are created by embedding watermarks in a transformed version of the original image. Some transforms and their strengths and weaknesses are discussed in the following sections.

Perception-wise, watermarking methods can be categorized as visible or invisible watermarks. Visible marks like logos placed in image corners serve content or copyright protection purposes. Invisible watermarks are essential for authentication, content integrity verification, and copyright protection.

Invisible watermarking falls into four groups[1]-[6]: fragile, semi-fragile, robust, and hybrid methods. Fragile methods are easily destroyed even with minor alterations and are useful for authentication and integrity verification. Semi-fragile methods protect data from intentional attacks but not from malicious ones. Robust techniques ensure copyright protection by withstanding various attacks.

Apart from those groupings, reversibility plays a crucial role in watermarking—reversible data hiding restores both the original multimedia file and the watermark perfectly without any distortion. This feature is vital for medical and military applications where accurate data retrieval is necessary.

Reversible methods not only recover hidden information but also ensure tamper-proofing and authentication in medical images embedding patient data and diagnostics without altering image quality for perfect recovery by medical professionals.

II. Literature Survey

Nguyen et al. proposed a method that limits the range of threshold values. Instead of brute-force searching of all the threshold values in the HPS method or choosing threshold values unsystematically, this technique classifies & selects a number of thresholds whose frequencies are used to satisfy the vital capacity & gain the best imperceptibility.

Wei Song et al delved into the importance of digital medical images. They highlighted that any alterations to these images could result in serious physiotherapy mishaps. Thus, safeguarding the genuineness and completeness of digital images is critical, necessitating the development of new methods to safeguard them. Digital watermarking, entailing implanting crucial data into the host multimedia, emerges as a viable approach for digital rights management, verification, and concealing data. In their study, the researchers explored the attributes of medical images and watermarking methods, presented a fundamental process for implementing these methods, and assessed the effectiveness of different algorithms.

Lendale et al introduced a novel authentication technique for medical images based on double watermarking technology. The advanced 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.

K. Pushpala worked on various watermarking techniques with a perspective of applying them to medical images that are stored on the PACS. It discusses the applicability of an invertible watermarking technique for ensuring the integrity of medical images. Alteration done to any of the watermarked DICOM (digital imaging and communications in medicine) images can be detected with high reliability using an invertible fragile watermarking system.

Alavi et al introduced a new digital multi-watermarking method for safeguarding medical images' copyrights and verifying their authenticity. In hospitals, maintaining strict security, confidentiality, and integrity of medical images is crucial to prevent unauthorized alterations and copying of sensitive medical data. Ensuring the protection of medical information is of utmost importance during image transmission and storage. When it comes to watermarking medical images, extra caution must be exercised to embed watermark information without compromising image quality, as any degradation lead to incorrect diagnoses

Coatrieux et al outlined the essential requirements for adopting such a system among medical professionals and its collaboration with existing security measures. They presented various scenarios highlighting its role in image authentication, tracing, ensuring patient record integrity.

Sun et al proposed a new robust digital image blind watermark scheme that is used to protect color medical images. In this scheme, K-L transform is applied to an RGB medical image and the binary watermark is embedded into low frequency sub-band of DWT of the principal component of medical images. The embedding positions are chosen according to the human visual system (HVS

Lendale et al detailed a careful implementation of robust pipeline in the domain of watermark based secure medical image transmission. The pipeline comprises of three stages, involving insertion of first watermark in the first stage and the second watermark in the second stage. Insertion of the watermark invokes a multi transform algorithm implemented in two steps.

KumarSing et al introduced a watermarking method that used the two most popular transform domain techniques, discrete wavelet transforms (DWT) and discrete cosine transform (DCT). In the embedding process, the cover medical image is divided into two separate parts, region of interest (ROI) and non region of interest

(NROI). For identity authentication purpose, multiple watermarks that contains both image and text are embedding into ROI and NROI part of the same cover media object respectively.

III. Proposed System

In response to the escalating threat of image forgery in digital media, this paper introduces a pioneering approach to authentication leveraging a fusion of half-toning and QR code composition. The essence of this method lies in combining these two distinct techniques to fortify the security and reliability of image authentication mechanisms. Initially, the image undergoes transformation through half-toning, converting it into a binary format while preserving critical features. Following this step, QR codes are strategically embedded within the image, encoding cryptographic data essential for authenticity verification. This integration not only bolsters security but also streamlines forgery detection through digital analysis. By embedding authentication directly into the image, this approach significantly reduces the vulnerability to tampering and manipulation, effectively safeguarding against malicious activities. Experimental findings validate the effectiveness and resilience of the proposed method in accurately detecting and verifying image authenticity, thereby offering a promising solution to combat image forgery across a spectrum of applications.

Modules

1. Image Preprocessing:

The initial step involves preprocessing the input image to enhance subsequent processing steps. RGB to grayscale conversion is performed to simplify the image representation, reducing it to a single channel. This conversion preserves important luminance information while reducing computational overhead.

2. Half-Toning:

Following preprocessing, the grayscale image undergoes halftoning to convert it into a binary representation. Halftoning techniques such as dithering or error diffusion are applied to achieve this conversion. By transforming pixel intensities into binary values, halftoning preserves crucial visual features while simplifying the image for further processing.

3. QR Code Composition:

In this module, cryptographic information necessary for authentication is encoded into QR codes. QR codes are generated and strategically placed within the binary image. Placement optimization techniques ensure that QR codes cover significant areas of the image, maximizing robustness against tampering and enabling efficient authentication.

4. Image Reconstruction:

Once QR codes are generated, they are overlaid onto the binary image. Careful consideration is given to the placement of QR codes to minimize distortion and maintain readability. By seamlessly integrating QR codes with the binary image, the reconstruction module ensures that authentication data is embedded directly into the visual content.

5. Authentication Data Embedding:

This module focuses on the seamless fusion of QR codes and the binary image. The encoded QR codes are strategically embedded within the binary image, ensuring that authentication data is securely integrated. This direct embedding mitigates the risk of tampering or manipulation, enhancing the overall security of the authentication mechanism.

6. Forgery Detection:

The final module involves the application of digital analysis techniques to detect and prevent forgery. Through comprehensive analysis of the binary image and embedded QR codes, anomalies indicative of tampering or manipulation are identified. This robust forgery detection mechanism ensures the integrity and authenticity of visual content, offering a reliable solution to combat image forgery in diverse applications.

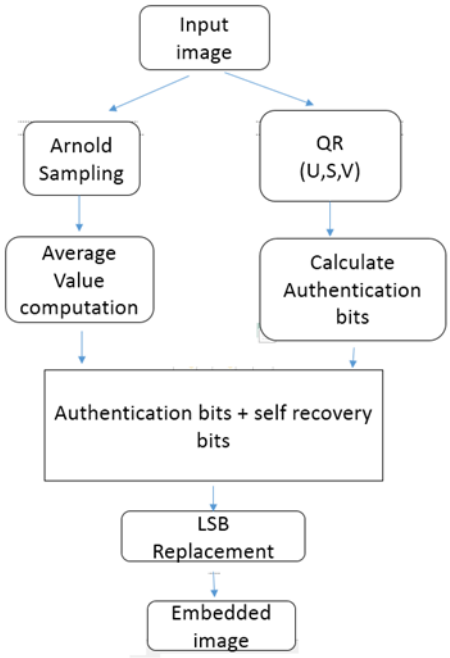

Fig 3.1 Proposed Architecture

The proposed scheme can effectively detect image tampering & recover the original image. The host image is divided into 4×4 blocks, & singular value decomposition (SVD) is then applied. It traces out block-wise SVD into the least significant bit (LSB) of the image pixels to determine the transformation in the original image. Two authentication bits - block authentication & self-recovery bits - are utilized as a preventive measure against vector quantization attack. The insertion of self-recovery bits is determined using Arnold transformation, which can recover the original image even after a high tampering rate. The SVD-based watermarking information enhances image authentication & provides a way to detect different attacked areas of the watermarked image.

In linear algebra, a **QR decomposition** (also called a **QR factorization**) of a matrix is a decomposition of a matrix *A* into a product *A* = *QR* of an orthogonal matrix *Q* and an upper triangular matrix *R*. QR decomposition is often used to solve the linear least squares problem and is the basis for a particular eigenvalue algorithm, the QR algorithm.

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 $Q\,Q^T = Q^T\,Q = 1$) and *R* is an upper triangular matrix (also called right triangular matrix). If *A* is invertible, the factorization is unique if 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, for any $1 \le k \le n$.[1] the first *k* columns of *Q* form an orthonormal basis for the span of the first *k* columns of *A* The triangular form of R arises because any column k of A depends only on the first k columns of Q.

3.2 Rectangular matrix

Generally speaking, we can factor a complex m×n matrix A, with m ≥ n, as the product of an m×m unitary matrix Q and an m×n upper triangular matrix R. Since the bottom (m−n) rows of an m×n upper triangular matrix are just zeroes, it's often useful to partition R, or both R and Q:

$$A = QR = Q\begin{bmatrix} R_1 \\ 0 \end{bmatrix} = [\,Q_1, Q_2\,]\begin{bmatrix} R_1 \\ 0 \end{bmatrix} = Q_1 R_1$$

Where R1 is an n×n upper triangular matrix, 0 is an (m − n)×n zero matrix, Q1 is m×n, Q2 is m×(m − n), and Q1 & Q2 both have orthogonal columns.

Golub & Van Loan (1996) refer to Q1R1 as the "thin QR factorization" of A; Trefethen and Bau call this the "reduced QR factorization".[1] If A is of full rank n & we require the diagonal elements of R1 to be

positive, then R1 and Q1 are unique, though Q2 may not be. R1 is then equal to the upper triangular factor of the Cholesky decomposition of A* A (= ATA if A is real).

QL, RQ and LQ decompositions

Analogously, we can define QL, RQ, & LQ decompositions, where L is a lower triangular matrix. There are several methods for computing the QR decomposition, such as the Gram–Schmidt process, Householder transformations, & Givens rotations. Each approach has its own set of advantages & disadvantages

Using the Gram–Schmidt process

Using the Gram–Schmidt process, let's consider its application to the columns of the full column rank A={a1,a2….,an} matrix, with the inner product (v,w) = (vT,w) (or v*,w for the complex case).

Define the projection:

$$\operatorname{proj}_{\mathbf{u}}\mathbf{a} = \frac{\langle \mathbf{u}, \mathbf{a} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle}\mathbf{u}$$

then:

$$\begin{aligned}
\mathbf{u}_1 &= \mathbf{a}_1, & \mathbf{e}_1 &= \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|} \\
\mathbf{u}_2 &= \mathbf{a}_2 - \operatorname{proj}_{\mathbf{u}_1}\mathbf{a}_2, & \mathbf{e}_2 &= \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|} \\
\mathbf{u}_3 &= \mathbf{a}_3 - \operatorname{proj}_{\mathbf{u}_1}\mathbf{a}_3 - \operatorname{proj}_{\mathbf{u}_2}\mathbf{a}_3, & \mathbf{e}_3 &= \frac{\mathbf{u}_3}{\|\mathbf{u}_3\|} \\
&\vdots & &\vdots \\
\mathbf{u}_k &= \mathbf{a}_k - \sum_{j=1}^{k-1} \operatorname{proj}_{\mathbf{u}_j}\mathbf{a}_k, & \mathbf{e}_k &= \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}
\end{aligned}$$

We can now express the our newly computed orthonormal basis:V

$$\begin{aligned}
\mathbf{a}_1 &= \langle \mathbf{e}_1, \mathbf{a}_1 \rangle \mathbf{e}_1 \\
\mathbf{a}_2 &= \langle \mathbf{e}_1, \mathbf{a}_2 \rangle \mathbf{e}_1 + \langle \mathbf{e}_2, \mathbf{a}_2 \rangle \mathbf{e}_2 \\
\mathbf{a}_3 &= \langle \mathbf{e}_1, \mathbf{a}_3 \rangle \mathbf{e}_1 + \langle \mathbf{e}_2, \mathbf{a}_3 \rangle \mathbf{e}_2 + \langle \mathbf{e}_3, \mathbf{a}_3 \rangle \mathbf{e}_3 \\
&\vdots \\
\mathbf{a}_k &= \sum_{j=1}^{k} \langle \mathbf{e}_j, \mathbf{a}_k \rangle \mathbf{e}_j
\end{aligned}$$

W.K.T

A =QR

Where

$$Q = [\mathbf{e}_1, \cdots, \mathbf{e}_n]$$

$$R = \begin{pmatrix} \langle \mathbf{e}_1, \mathbf{a}_1 \rangle & \langle \mathbf{e}_1, \mathbf{a}_2 \rangle & \langle \mathbf{e}_1, \mathbf{a}_3 \rangle & \cdots \\ 0 & \langle \mathbf{e}_2, \mathbf{a}_2 \rangle & \langle \mathbf{e}_2, \mathbf{a}_3 \rangle & \cdots \\ 0 & 0 & \langle \mathbf{e}_3, \mathbf{a}_3 \rangle & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

IV. Results & Discussion

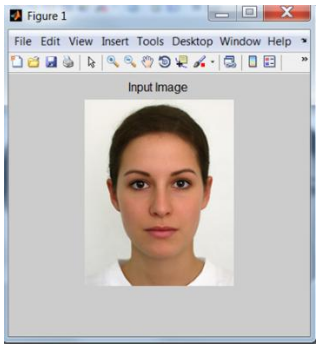

Fig 4.1. Input Image

Above figure 4.1 shows input image from data set in this stage image converted into gray scale image and resized to required stage

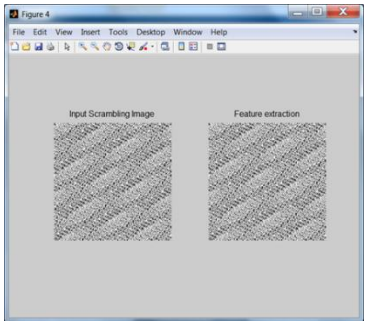

Fig 4.2 Scrambled and Feature extracted image

Above figure 4.2 shows scrambled image and feature extracted image for our embedding process. In this stage image authentication bits are identified using Arnold sampling

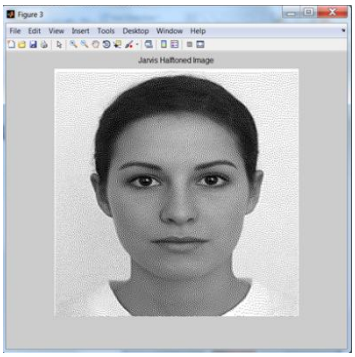

Fig 4.3 Halftoning image

Above figure 4.3 shows creating the illusion of continuous output with a binary device

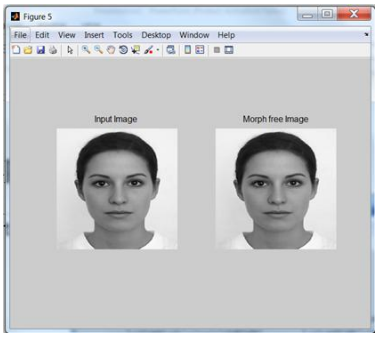

Figure 4.4 Input and Morph free Image

Above figure 4.4 shows final morph free image in our embedding process.

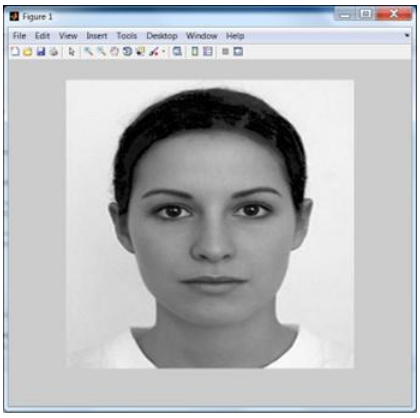

Fig 4.5 Received Image

Above figure 4.5 shows received image after performing morphing

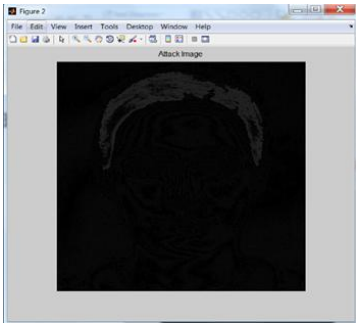

Fig 4.6Attack detected Image

Above figure 4.6 shows tamper identified image using our authentication bits

Fig 4.7 Recovered Image

Above figure 4.7 shows recovered image by performing LU decomposition

Performance evaluation

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

TABLE 4.1 **SNR Calculation**

S.No	Image set	EXISTING APPROCH - PSNR	PROPOSED APPROCH - PSNR
1	1	50.2302	58.23
2	2	51.0662	56.4
3	3	51.1394	55.8
4	4	50.7783	63.8

V. Conclusion

In this work, we have proposed a fast and effective keypoint-based copy-move forgery detection and localization technique. The research introduces a QR-based fragile watermarking plan utilizing a grouped block method for enhanced security and an extra means to pinpoint the tampered areas in various medical images. To withstand the vector quantization attack, two verification bits - block authentication and self-recovery bits - were applied. The inclusion of the Arnold transform enables recovery of the altered region from adjacent blocks, leading to increased NCC and PSNR of the recuperated host image.

References

[1] Muhammad Sajjad, Khan Muhammad, Sung Wook Baik, Seungmin Rho, Zahoor Jan, Sang-Soo Yeo, Irfan Mehmood, 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, Irfan Mehmood, Seungmin Rho, Sung Wook Baik, 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.
[15] MINERVA M YEUNG AND FRED MINTZER. An Invisible Watermarking Technique For Image Verification. In Image Processing, 1997. Proceedings, International Conference On, Volume 2, Pages 680– 683. IEEE, 1997.
[16] S. WALTON. Information Authentication For A Slippery New Age. 1995.