A Dissertation Report on

Data Hiding for Image Authentication Using Secrete Sharing for Color Images

Submitted by

Mr.Sandip A.More

Under the Guidance of

Dr.S.P.Sonavane

In the partial fulfillment for the award of

Master of Technology
in
Computer Science and Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

2014-15

CERTIFICATE

Walchand College of Engineering,Sangli.
2014-2015

This is to certify that the dissertation entitled,

Data Hiding for Image Authentication Using Secrete Sharing for Color Images

has been carried out by

Mr.Sandip A.More

In the partial fulfillment for the award of

MASTER OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING.

This dissertation is a record of students own work carried out by him during the academic year 2014-2015, as per the curriculum laid down by

Shivaji University,Kolhapur.

Dr.S.P.Sonavane
Project Guide

Dr.B.F.Momin
Head of the Department

Prof.S.N.Kore
Dean Academics

Acknowledgement

I would like to express my deep sense of gratitude towards my guide **Dr.S.P.Sonavane**, for her valuable help and guidance for the project. I am highly indebted to her for constantly encouraging me by giving critics on my work.

I express gratitude towards **Dr.B.F.Momin,** HOD, Computer Science & Engineering Department for providing the support and giving me his valuable time.

I also express gratitude towards **my family members**, and **my friends** for encouraging me with their valuable suggestions and motivating me from time to time.

Mr.Sandip A. More
M.Tech.(CSE)

Declaration

I, the undersigned hereby declare that the dissertation entitled **"Data Hiding for Image Authentication Using Secrete Sharing for Color Images"** submitted by me to Walchand College of Engineering , Sangli, for the award of the degree of Master of Technology in Computer Science and Engineering, under the guidance of **Dr.S.P.Sonavane** is my original work.

I further declare that to the best of my knowledge and belief, this work has not been previously submitted to this or any other university.

Mr.Sandip.A.More
M.Tech. (CSE)
Walchand College of Engineering, Sangli.

Contents

List of Figures

List of Tables

A

SYNOPSIS

of

The Dissertation Work

on

Data Hiding for Image Authentication Using Secret Sharing for Color images

for

M.Tech. in Computer Science and Engineering

at

Department of CSE,
Walchand College of Engineering,
Sangli.
(An Autonomous Institute)

by

Mr. S. A. More

Guide

Dr. S. P. Sonavane.

Academic Year

2014-15

- **Name of College:** Walchand College of Engineering, Sangli.
- **Name of Course:** M.Tech. CSE.
- **Name of the Student:** Mr. S. A. More
- **Date of Re-Registration:** August 2013
- **Name of the Guide:** Dr. S. P. Sonavane.
- **Title:** "Data Hiding for Image Authentication Using Secret Sharing for Color images"

1 Introduction

Image authentication and self-repair capabilities are useful for the security protection of digital documents in many fields, such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments,and so on.

Most of methods proposed in past embed authentication signal and self-repairing data into cover image itself making it inefficient if cover image itself is destroyed. For the self-repairing of tampered data at attacked image parts the original image data to help in self-repairing needs to be embedded somewhere else without altering the cover image itself. The alpha channel of the color image can be a used to carry authentication signal and data for self-repairing computed from original mage.

A new approach is proposed to color image authentication with authentication data recovery capability and security enhancement but without any perceptible distortion. In the proposed method, the secret sharing scheme is used to carry authentication signals ,image content data and shares to help recover tampered authentication data. A color image is created from a document image with an alpha channel plane. The original color image is binarised by moment-preserving thresholding. Data for authentication and recovery are computed from each block of binarised image and taken as input to the secret sharing scheme to generate secret shares. The share values are subsequently mapped into a small range of alpha channel values (238 - 254) near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of security protection and authentication data repair capabilities. In authentication process authentication signal extracted from each block of alpha channel plane of stego image by using inverse secret

sharing scheme are compared with authentication signal computed from corresponding block of binarised version of stego image. The block is marked as tampered if match is not found and authentication data recovery is applied to the tampered block by secrete recovery scheme after collecting two shares from unmarked blocks.

2 Relevance/Motivation

The problem encountered in the image authentication and the self-recovery capability for the original image data under possible attack are summarized as below

1. The original data of the cover image are embedded into the image itself for use in later data recovery, the cover image is destroyed in the first place and the original data are no longer available for data recovery, resulting in a contradiction.
2. The data to be embedded in the carrier are often large sized resulting in distortion of original image.
3. Conventionally, the concepts of secret sharing and data hiding for image authentication are two irrelevant issues in the domain of information security.

To overcome above mentioned problems a proposed system utilizes the extra alpha channel in a color image to embed the original image content data and authentication signals and also secret shares to help recover tampered authentication data.

3 Literature Review

Some of research on image authentication and data repairing is given below

Recently Che-Wei, Lee [1] have proposed image authentication and fidelity for binary like grayscale images by embedding authentication signal and repairing data into alpha component of PNG images.Wu and Liu [2] manipulated the so-called flippable pixels to create specific relationships to embed data for authentication and annotation of binary images.

H. Yang and Kot [3] proposed a two-layer binary image authentication method in which one layer is used for checking the image fidelity and the other for checking image integrity. In H. Yang and A. C. Kot [4], a set of pseudo random pixels in a binary or half tone image are chosen and cleared, and authentication codes are accordingly computed and inserted into selected random pixels. In Tzeng and Tsai's [5] method, randomly generated authentication codes are embedded into image blocks for use in image authentication, and a so-called code holder is used to reduce image distortion resulting from data embedding

Lee et al. [6] proposed a Hamming-code-based data embedding method that flips one pixel in each binary image block for embedding a watermark,yielding small distortions and low false negative rates. Lee et al.[7] improved the method later by using an edge line similarity measure to select flippable pixels for the purpose of reducing the distortion.

4 Proposed Work

4.1 Scope:

Based on above discussion proposed work is to implement and analyze blind authentication method based on the secret sharing technique with a authentication data recovery capability for color document images.

Objectives of proposed work are as follows:

- To generate an authentication signal for each block of a color document image using Shamir Secret Sharing.
- Formation of color image by combining the alpha channel plane with the original color image
- To embed authentication signal into alpha channel of color image to yield a transparent stego-image with a disguise effect
- To implement the image authentication process to mark image block as tampered or not.
- To Implement authentication data recovery process to each tampered block using reverse Shamir Secret Sharing.
- To analyse and compare with other document image authentication methods with respect to - distortion in stego image,recovery capability,authentication precision and distortion of authenticated image parts.

4.2 Methodology:

4.2.1 System architecture

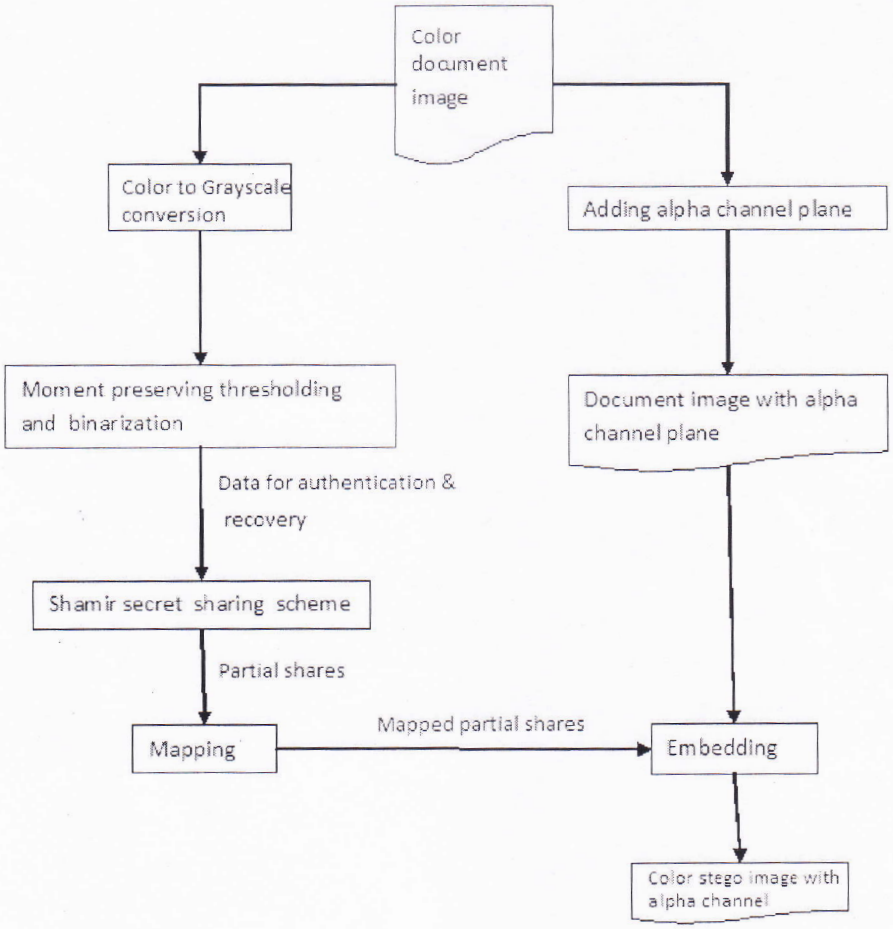


Figure 1: Creating a color image with alpha channel and generation and embedding of data into alpha channel

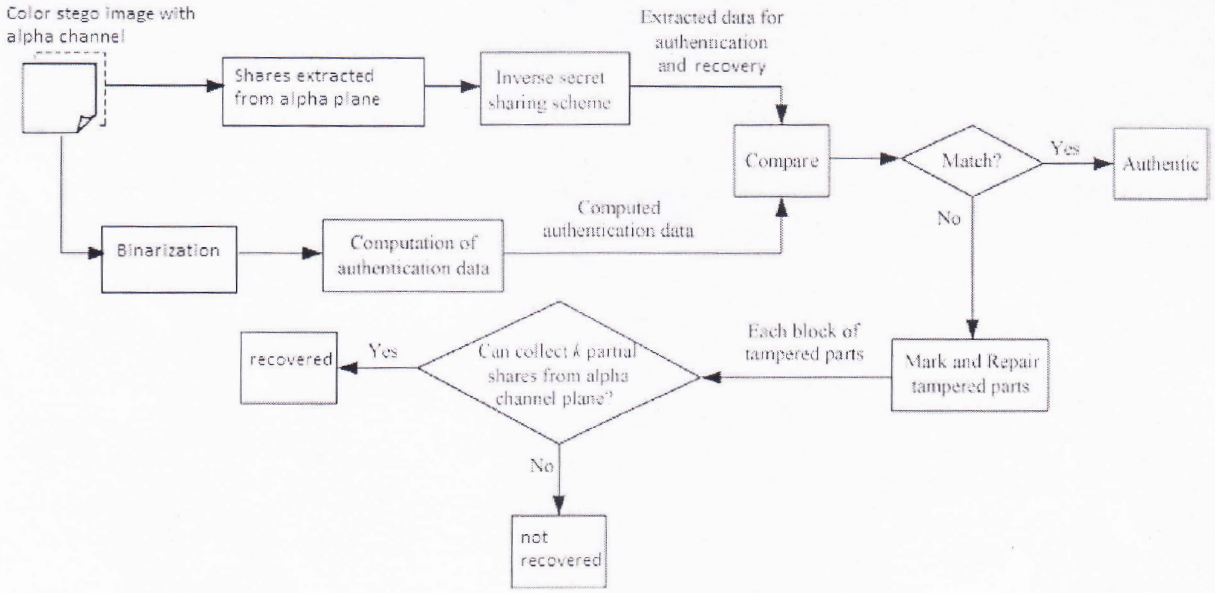


Figure 2: Authentication process including verification and recovery of authentication data.

4.2.2 Module 1:(k, n)-threshold secret sharing

Input: Secret d in the form of an integer, number n of shares, and threshold $k \leq n$.

Output: n shares in the form of integers for the n participants to keep.

4.2.3 Module 2: Secret recovery

Input: k shares collected from the participants and the prime number p with both k and p being those used in module 1.

Output: Secret hidden in the shares and coefficients used in module 1.

4.2.4 Module 3: Generation of a color stego-image with a alpha channel from a given color image.

Input: A color document image I with two major gray values and a secret key K.

Output: Color Stego-image with relevant data embedded, including the authentication signals and the data used for recovery in alpha channel.

4.2.5 Module 4: Authentication of a given color stego-image with alpha channel.

Input: stego-image I and the secret key K used in module 3.

Output: image with tampered blocks marked and their authentication data repaired if possible.

4.3 System Requirement

Hardware Requirement

- Processor - Pentium -I5
- Speed - 2.6 Ghz
- RAM - 2 GB
- Hard Disk - 500 GB

Software Requirement

- Operating System -2000/XP/windows 7
- Programming Languages - Matlab,Java
- Tool - IDE Netbeans.

References

[1] Che-Wei Lee and Wen-Hsiang Tsai, "A Secret-Sharing-Based Method for Authentication Of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability," *IEEE transactions on image processing*, vol. 21, no. 1, January 2012.

[2] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528-538,Aug. 2004.*

[3] H. Yang and A. C. Kot "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Process.Lett., vol. 13, no. 12, pp. 741-744, Dec.2006.*

[4] H. Yang and A. C. Kot "Pattern-based data hiding for binary images authentication by connectivity-preserving," *IEEE Trans. Multimedia,vol. 9, no. 3, pp. 475-486, Apr. 2007.*

[5] C. H. Tzeng and W. H. Tsai "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement," *IEEE Commun. Lett., vol. 7, no. 9, pp.443-445, Sep. 2003.*

[6] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon "A new binary image authentication scheme with small distortion and low false negative rates," *IEICE Trans. Commun., vol. E90-B, no. 11, pp. 3259-3262, Nov. 2007.*

[7] Y. Lee, H. Kim, and Y. Park "A new data hiding scheme for binary image authentication with small image distortion," *Inf. Sci., vol. 179,no. 22, pp. 3866-3884, Nov. 2009.*

Date: 28/8/13

Place: Sangli.

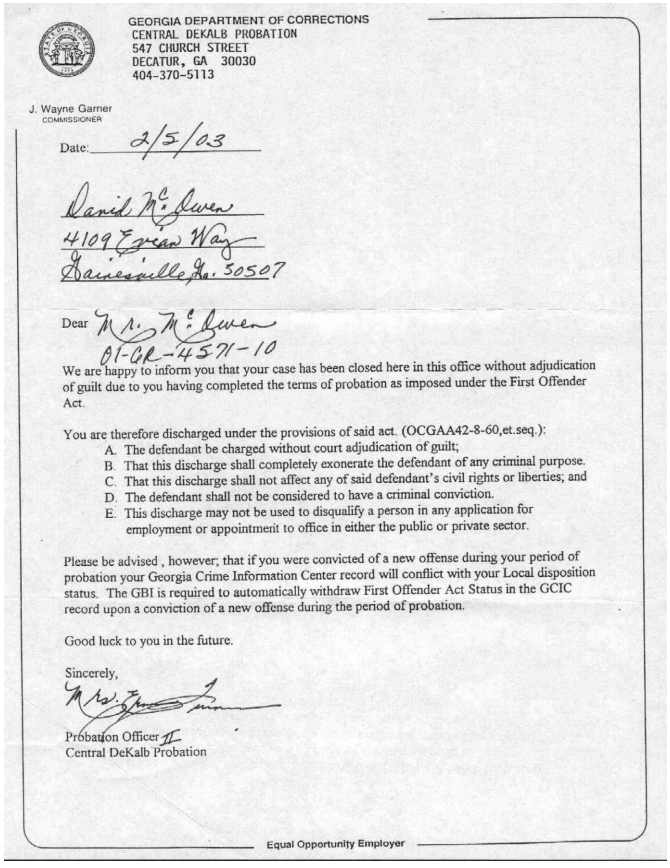
Mr.S.A.More
Student

Prof. Dr. S.P.Sonavane
Guide

Prof. Dr. B. F. Momin
HOD
Department of CSE ,
Walchand College of Engineering ,
Sangli.

Chapter 1

Introduction



GEORGIA DEPARTMENT OF CORRECTIONS
CENTRAL DEKALB PROBATION
547 CHURCH STREET
DECATUR, GA 30030
404-370-5113

J. Wayne Garner
COMMISSIONER

Date: 2/5/03

David McOwen
4109 Tyson Way
Dawsonville Ga. 30507

Dear Mr. McOwen
01-CR-4571-10

We are happy to inform you that your case has been closed here in this office without adjudication of guilt due to you having completed the terms of probation as imposed under the First Offender Act.

You are therefore discharged under the provisions of said act. (OCGAA42-8-60,et.seq.):

A. The defendant be charged without court adjudication of guilt;
B. That this discharge shall completely exonerate the defendant of any criminal purpose.
C. That this discharge shall not affect any of said defendant's civil rights or liberties; and
D. The defendant shall not be considered to have a criminal conviction.
E. This discharge may not be used to disqualify a person in any application for employment or appointment to office in either the public or private sector.

Please be advised , however; that if you were convicted of a new offense during your period of probation your Georgia Crime Information Center record will conflict with your Local disposition status. The GBI is required to automatically withdraw First Offender Act Status in the GCIC record upon a conviction of a new offense during the period of probation.

Good luck to you in the future.

Sincerely,

Probation Officer II
Central DeKalb Probation

Equal Opportunity Employer

Figure 1.1: Scanned Legal document

Digital image is a form for preserving important information. However, with the fast advance of digital technologies, it is easy to make visually imperceptible modifications to the contents of digital images. How to ensure the integrity and the authenticity of a digital image is thus a challenge. It is desirable to design effective methods to solve this kind of image authentication problem [1]-[3], particularly for images of documents whose security must be protected. It is also hoped that,if part of a document image is verified to have been illicitly altered, the destroyed content can be repaired. Such image content authentication and self-repair capabilities are useful for the security protection of digital documents in many fields, such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on.

Document images, which include texts, tables, line arts, etc., as main contents, are often digitized into grayscale images with two major gray values, one being of the background (including mainly blank spaces) and the other of the foreground (including mainly texts). It is noted that such images, although gray valued in nature, look like binary. For example, the two major gray values in the document image shown in Fig.1.1 are 174 and 236, respectively. It seems that such binary-like grayscale document images may be thresholded into binary ones for later processing, but such a thresholding operation often destroys the smoothness of the boundaries of text characters, resulting in visually unpleasant stroke appearances with zigzag contours. Therefore,in practical applications, text documents are often digitized and kept as grayscale images for later visual inspection.

In general, the image authentication problem is difficult for a binary document image because of its simple binary nature that leads to perceptible changes after authentication signals are embedded in the image pixels. Such changes will arouse possible suspicions from attackers. A good solution to such binary image authentication should thus take into account not only the security issue of preventing image tampering but also the necessity of keeping the visual quality of the resulting image. In this paper, we propose an authentication method that deals with binary-like grayscale document images instead of pure binary ones and simultaneously solves the problems of image tampering detection and visual quality

keeping.

In this dissertation work, a method for the authentication of document images with an additional self-repair capability for fixing tampered image data is explored. The input cover image is assumed to be a binary-like grayscale image with two major gray values like the one shown in Fig.1.1. After the explored method is applied, the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format with an additional alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be verified by the explored method for its authenticity. Integrity modifications of the stego-image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is totally removed from the stego-image, the entire resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The explored method is based on the so-called $(k, n)-$ threshold secret sharing scheme explored by Shamir [11] in which a secret message is transformed into n shares for keeping by participants, and when k of n the shares, not necessarily all of them, are collected, the secret message can be losslessly recovered. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

Conventionally, the concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security. However, in the explored method, we combine them together to develop a new image authentication technique. The secret sharing scheme is used in the developed technique not only to carry authentication signals and image content data but also to help repair tampered data through the use of shares.

An issue in the self-repairing of tampered data at attacked image parts is that, after the original data of the cover image are embedded into the image itself for use in later data repairing, the cover image is destroyed in the first place and the original data are no longer available for data repairing, resulting in a contradiction. A solution to this problem is to embed the original image data somewhere else without altering the cover image itself. The

way explored in this dissertation work is to implement this solution that utilize the extra alpha channel in a PNG image to embed the original image data. However, the alpha channel of the PNG image is originally used for creating a desired degree of transparency for the image. Moreover, embedding of data into the alpha channel will create random transparency in the resulting PNG image, producing an undesirable opaque effect. One way out, as explored in this thesis, is to map the resulting alpha channel values into a small range near their extreme value of 255, yielding a nearly imperceptible transparency effect on the alpha channel plane.

Another problem encountered in the self-repairing of the original image data is that the data to be embedded in the carrier are often large sized. For our case here with the alpha channel as the carrier, this is not a problem because the cover image that we deal with is essentially binary-like, and thus, we may just embed into the carrier a binary version of the cover image, which includes much less data.

Furthermore, through a careful design of authentication signals, a proper choice of the basic authentication unit (i.e., the unit of 2x3 image block) and a good adjustment of the parameters in the Shamir scheme, we can reduce the data volume of the generated shares effectively so that more shares can be embedded into the alpha channel plane. The larger the number of shares is, the higher the resulting data repair capability becomes, as shown in the subsequent sections. Finally, we distribute the multiple shares randomly into the alpha channel to allow the share data to have large chances to survive attacks and to thus promote the data repair capability. This is the secret-sharing-based authentication method for binary-like grayscale document images. This is an authentication method for such document images through the use of the PNG image. Note that this method is not a secret sharing technique but a document image authentication method.

Chapter 2

Literature Survey

Several methods for binary image authentication have been in the past. Wu and Liu [4] manipulated the so called flippable pixels to create specific relationships to embed data for authentication and annotation of binary images. Yang and Kot [5] proposed a two layer binary image authentication method in which one layer is used for checking the image fidelity and the other for checking image integrity. In the method, a connectivity preserving transition criterion for determining the flippability of a pixel is used for embedding the cryptographic signature and the block identifier. Later, Yang and Kot [6] proposed a pattern-based data hiding method for binary image authentication in which three transition criteria are used to determine the flippabilities of pixels in each block, and the watermark is adaptively embedded into embeddable blocks to deal with the uneven embeddability condition in the host image. In the method proposed in [7], a set of pseudorandom pixels in a binary or halftone image are chosen and cleared, and authentication codes are accordingly computed and inserted into selected random pixels.

In Tzeng and Tsai's method [8],randomly generated authentication codes are embedded into image blocks for use in image authentication, and a so-called code holder is used to reduce image distortion resulting from data embedding.Lee et al.[9] proposed a Hamming-code-based data embedding method that flips one pixel in each binary image block for embedding a watermark, yielding small distortions and low false negative rates. Lee et al. [10] improved the method later by using an edge line similarity measure to select flippable

pixels for the purpose of reducing the distortion.

Chapter 3

Relevance and Motivation for Work

The image authentication problem is difficult for a binary document image because of its simple binary nature that leads to perceptible changes after authentication signals are embedded in the image pixels. Such changes will arouse possible suspicions from attackers. A good solution to such binary image authentication should thus take into account not only the security issue of preventing image tampering but also the necessity of keeping the visual quality of the resulting image. There is a need of authentication method that deals with binary-like grayscale document images instead of pure binary ones and simultaneously solves the problems of image tampering detection and visual quality keeping.This method for the authentication of document images should also have an additional self-repair capability for fixing tampered image data.

Conventionally, the concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security. Hence the new method must combine them together to develop a new image authentication technique. The secret sharing scheme is used in the developed technique not only to carry authentication signals and image content data but also to help repair tampered data through the use of shares.

An issue in the self-repairing of tampered data at attacked image parts is that, after the original data of the cover image are embedded into the image itself for use in later data repairing, the cover image is destroyed in the first place and the original data are no longer

available for data repairing, resulting in a contradiction. A solution to this problem is to embed the original image data somewhere else without altering the cover image itself. The way explored in this dissertation work to implement this solution is to utilize the extra alpha channel in a PNG image to embed the original image data. However, the alpha channel of the PNG image is originally used for creating a desired degree of transparency for the image. Moreover, embedding of data into the alpha channel will create random transparency in the resulting PNG image, producing an undesirable opaque effect. One solution is to map the resulting alpha channel values into a small range near their extreme value of 255, yielding a nearly imperceptible transparency effect on the alpha channel plane.

Another problem encountered in the self-repairing of the original image data is that the data to be embedded in the carrier are often large sized. For our case here with the alpha channel as the carrier, this is not a problem because the cover image that we deal with is essentially binary-like, and thus, we may just embed into the carrier a binary version of the cover image, which includes much less data. Furthermore, through a careful design of authentication signals, a proper choice of the basic authentication unit (i.e., the unit of 2x3 image block) and a good adjustment of the parameters in the Shamir scheme, we can reduce the data volume of the generated shares effectively so that more shares can be embedded into the alpha channel plane. It is noted that, the larger the number of shares is, the higher the resulting data repair capability becomes. Finally the multiple shares are randomly distributed into the alpha channel to allow the share data to have large chances to survive attacks and to thus promote the data repair capability. The explored method is the unique secret-sharing-based authentication method for binary-like grayscale document images. It is also the differnet authentication method for such document images through the use of the PNG image. Note that this method is not a secret-sharing technique but a document image authentication method.

Chapter 4

Shamir Secret Sharing

4.1 Introduction

Shamir[11] show how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

Shamir generalize the problem to one in which the secret is some data D (e.g., the safe combination) and in which nonmechanical solutions (which manipulates this data) are also allowed. The goal is to divide D into $D_1, D_2, ..., D_n$ in such a way that

1. knowledge of any k or more $D_i$pieces makes D easily computable;
2. knowledge of any k-1 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Such a scheme is called a (k, n) threshold scheme.

4.2 Applications of Secret Sharing

Efficient threshold schemes can be very helpful in the management of cryptographic keys. In order to protect data we can encrypt it, but in order to protect the encryption key we need a different method (further encryptions change the problem rather than solve it). The most secure key management scheme keeps the key in a single, well-guarded location (a computer, a human brain, or a safe). This scheme is highly unreliable since a single misfortune (a computer breakdown, sudden death, or sabotage) can make the information inaccessible. An obvious solution is to store multiple copies of the key at different locations, but this increases the danger of security breaches (computer penetration betrayal, or human errors). By using a (k, n) threshold scheme with $n = 2k - 1$ we get a very robust key management scheme: We can recover the original key even when $\lceil n/2 \rceil = k - 1$ of the n pieces are destroyed, but our opponents cannot reconstruct the key even when security breaches expose $\lceil n/2 \rceil = k - 1$ of the remaining k pieces.

In other applications the tradeoff is not between secrecy and reliability, but between safety and convenience of use. Consider, for example, a company that digitally signs all its checks. If each executive is given a copy of the company's secret signature key, the system is convenient but easy to misuse. If the cooperation of all the company's executives is necessary in order to sign each check, the system is safe but in-convenient. The standard solution requires at least three signatures per check, and it is easy to implement with a (3, n) threshold scheme. Each executive is given a small magnetic card with one D_i piece, and the company's signature generating device accepts any three of them in order to generate (and later destroy) a temporary copy of the actual signature key D. The device does not contain any secret information and thus it need not be protected against inspection. An unfaithful executive must have at least two accomplices in order to forge the company's signature in this scheme.

Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate. Ideally we would like the cooperation to be based on mutual consent, but the veto power this mechanism gives to each member can paralyze the activities of the group. By properly choosing the k and n

parameters we can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it.

4.3 A simple (k-n) Threshold Scheme

Shamir scheme is based on polynomial interpolation: Given k points in the 2-dimensional plane $(x_1, y_1), (x_2, y_2), ..., (x_k, y_k)$ with distinct x_i' s, there is one and only one polynomial q(x) of degree $k-1$ such that $q(x) = y_i$ for all i. Without loss of generality, we can assume that the data D is (or can be made) a number. To divide D into pieces, we pick a random $k-1$ degree polynomial $q(x) = a_0 + a_1 x + ... + a_{k-1}x^{k-1}$ in which $a_0 = D$ and evaluate: $D_1 = q(1), D_2 = q(2), ..., D_i = q(i), ..., D_n = q(n)$. Given any subset of k of these D_i values (together with their identifying indices), we can find the coefficients of q(x) by interpolation, and then evaluate $D = q(0)$. Knowledge of just $k-1$ of these values, on the other hand, does not suffice in order to calculate D.

To make this claim more precise, we use modular arithmetic instead of real arithmetic. The set of integers modulo a prime number p forms a field in which interpolation is possible. Given an integer valued data D, we pick a prime p which is bigger than both D and n. The coefficients $a_1, a_2, ..., a_{k-1}$ in q(x) are randomly chosen from a uniform distribution over the integers in $[0, p)$, and the values $D_1, D_1, ..., D_n$ are computed modulo p.

Let us now assume that k - 1 of these n pieces are revealed to an opponent. For each candidate value D' in $[0, p)$ he can construct one and only one polynomial $q'(x)$ of degree $k-1$ such that $q'(0) = D'$ and $q'(i) = D_i$ for the $k-1$ given arguments. By construction, these p possible polynomials are equally likely, and thus there is abolutely nothing the opponent can deduce about the real value of D. Efficient $O(nlog2n)$ algorithms for polynomial evaluation and interpolation have been proposed in past, but even the straightforward quadratic algorithms are fast enough for practical key management schemes. If the number D is long, it is advisable to break it into shorter blocks of bits (which are handled separately) in order to avoid multiprecision arithmetic operations. The blocks cannot be arbitrarily short, since

the smallest usable value of p is n + 1 (there must be at least n + 1 distinct arguments in [0, p) to evaluate q(x) at). However, this is not a severe limitation since sixteen bit modulus (which can be handled by a cheap sixteen bit arithmetic unit) suffices for applications with up to 64,000 D_i pieces.

4.4 Properties of (k-n) Threshold Scheme

Some of the useful properties of this (k, n) threshold scheme (when compared to the mechanical locks and keys solutions) are:

1. The size of each piece does not exceed the size of the original data.

2. When k is kept fixed, D pieces can be dynamically added or deleted (e.g., when executives join or leave the company) without affecting the other D_i pieces. (A piece is deleted only when a leaving executive makes it completely inaccessible, even to himself.)

3. It is easy to change the D_i pieces without changing the original data D;all we need is a new polynomial q(x) with the same free term. A frequent change of this type can greatly enhance security since the pieces exposed by security breaches cannot be accumulated unless all of them are values of the same edition of the q(x) polynomial.

4. By using tuples of polynomial values as Di pieces, we can get a hierarchical scheme in which the number of pieces needed to determine D depends on their importance. For example, if we give the company's president three values of q(x), each vice-president two values of q(x), and each executive one value of q(x), then a (3, n) threshold scheme enables checks to be signed either by any three executives, or by any two executives one of whom is a vice-president, or by the president alone.

Chapter 5

Image Authentication and Data Repairing

5.1 Image Authentication

Image authentication is the process of proving image identity and authenticity. Digital images are increasingly transmitted over non-secure channels such as the Internet. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Nowadays image authentication techniques have recently gained great attention due to its importance of multimedia applications. The traditional cryptographic hash functions, such as MD5 and SHA-1 are used for authentication. However, these hash functions are not suitable for image authentication. Because they are so sensitive that even one bit change of the input data will lead to a significant change of the output hash. Besides, image authentication system requires the main content sensitive. In order to make up for the disadvantage of the traditional cryptographic hash functions in image authentication, robust image hashing was first introduced which provide good ROC performance, low collision probability.

5.2 Image Authentication Requirements

1. **Sensitivity:** The authentication system must be able to detect any content modification or manipulation. For any authentication algorithms, detection of any manipulation is required and not only content modification.
2. **Robustness:** The authentication system must tolerate content preserving manipulations.
3. **Localization:** The authentication system must be able to locate the image regions that have been altered.
4. **Recovery:** The authentication system must be able to partially or completely restore the image regions that were tampered.
5. **Security:** The authentication system must have the capacity to protect the authentication data against any falsification attempts.

5.3 Methods of Image Authentication

The major techniques for authenticating an image are as follows,

1. **Watermarking based authentication:**

   Digital watermarking is the art and science of embedding copyright information in the files; the information which is embedded in files is called watermarks. Digital watermark is one of the signals which are added to a document to authenticate it and to prove the ownership. Two approaches for watermarking authentication are possible- fragile watermarking and robust watermarking.

   Advantages of watermarking based authentication:

   - Uniquely identify the author of copyright work.
   - Implementation on pc platform is possible.

- Embedding watermarks is easy.
- Image tampering detection.

Disadvantages of watermarking based authentication:

- Doesnt prevent image copying.
- Watermark vanishes if someone manipulates the image.
- Resizing, compressing images from one file type to another may diminish the watermark and it becomes unreadable.

2. **Cryptography based authentication:**

Cryptography is the science of transforming the documents or images. It includes two functions encryption and decryption. Algorithms based on conventional cryptography show satisfying results for image authentication with high tamper detection. Localization performances are not very good but may be acceptable for some applications. Even a small change in the image pixels or even in the binary image data causes changes because the hash function is very sensitive. The image is classified as manipulated, when just only one bit of this image is changed; this is very severe for most of applications.

Advantages of Cryptography based authentication:

- Conventional cryptography show satisfying results for image
- authentication with high tamper detection.

Drawbacks of Cryptography based authentication:

- Localization performances are not very good.
- Hash functions are very sensitive.
- Knowledge of private key
- Different to distinguish between malicious and innocuous modification

- Delay in transmission

3. **Robust image hashing authentication:**

Perceptual hash function (PHF) extract a set of features from the image to form a compact representation which can be used for authentication. Robustness, fragility and security are the three key issues of image hashing. Robustness requires that image hashing should be invariant to incidental modifications, such as JPEG compression, blur, noise, enhancement and some other perceptually similar operations. Fragility means that the image hashing should have the ability to distinguish the visually distinct images. Security is the degree to prevent the attacker from tricking the authentication system with a maliciously tampered image. A robust and secure image hashes using Zernike moments, is based on rotation invariance of magnitudes. In image processing, orthogonal rotation-invariant moments (ORIMs) can effectively catch important information in an image.

Advantages of image hashing authentication:

- Hashes produced are robust against common image processing operations including brightness adjustment, scaling, small angle rotation, JPEG coding and noise contamination.
- Collision probability between hashes of different images is very low.
- Reasonably short hash length and good ROC performance.

Chapter 6

Problem Definition

Ensuring the integrity and the authenticity of a digital image is a challenge for images of documents whose security must be protected. It is also important to verify if part of a document image have been illicitly altered, and to repaire the altered content. Such image content authentication and self-repair capabilities are useful for the security protection.

In this dissertation work, a method for the authentication of document images with an additional self-repair capability for fixing tampered image data is explored. The input cover image is assumed to be a binary-like grayscale image with two major gray values like the one shown in Fig.1.1. After the explored method is applied, the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format with an additional alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be verified by the explored method for its authenticity. Integrity modifications of the stego-image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is totally removed from the stego-image, the entire resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The explored method is based on the so-called $(k, n)-$ threshold secret sharing scheme proposed by Shamir [11] in which a secret message is transformed into n shares for keeping by participants, and when k of n the shares, not necessarily all of them, are collected, the secret message can be losslessly recovered. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

Conventionally, the concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security. However, in the explored method, we combine them together to develop a new image authentication technique. The secret sharing scheme is used in the developed technique not only to carry authentication signals and image content data but also to help repair tampered data through the use of shares.

An issue in the self-repairing of tampered data at attacked image parts is that, after the original data of the cover image are embedded into the image itself for use in later data repairing, the cover image is destroyed in the first place and the original data are no longer available for data repairing, resulting in a contradiction. A solution to this problem is to embed the original image data somewhere else without altering the cover image itself. The way explored in this dissertation work is to implement this solution that utilize the extra alpha channel in a PNG image to embed the original image data. However, the alpha channel of the PNG image is originally used for creating a desired degree of transparency for the image. Moreover, embedding of data into the alpha channel will create random transparency in the resulting PNG image, producing an undesirable opaque effect. One way out, as explored in this thesis, is to map the resulting alpha channel values into a small range near their extreme value of 255, yielding a nearly imperceptible transparency effect on the alpha channel plane.

We will also explore the possible extension of the method for color images. Specifically, PNG image is created from a color document image with an alpha channel plane. The original image I has three grayscale channel planes-red,green and blue. Next, each red,green and blue component is binarized by moment-preserving thresholding [13], yielding a binary version of I . Data for authentication and repairing are then computed from binary versions of red,green and blue components and taken as input to the Shamir secret sharing scheme to generate secret shares separately. The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares generated from red plane are randomly embedded

into the alpha channel of original color image I for the purpose of promoting the security protection and data repair capabilities. Secrete shares generated from each of red,green and blue components of original color image I are embedded into red,green and blue components respectively of a new color image(an authentication color image). Since the alpha channel plane is used for carrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication.

Chapter 7

Proposed Work

7.1 Scope

Based on above discussion proposed work is to implement and analyze blind image authentication method based on the secret sharing technique with a data repair capability for binary-like grayscale document images via the use of the alpha plane of images.

We will also explore the possible extension of the proposed method for color images.The extended authentication method for color images is also based on the above mentioned secret sharing technique with a data repair capability and it uses the authentication image instead of a single alpha plane and hence it is a non-blind authentication method.

7.2 Objectives of Proposed Work

7.2.1 Objectives of proposed work for grayscale images

- To generate an authentication signal for each block of a grayscale document image.
- To form PNG image by combining the alpha channel plane with the original grayscale image
- To embed authentication signal into alpha channel of PNG image to yield a transparent stego-image with a disguise effect

- To implement the image authentication process to mark image block as tampered or not.
- To implement data repairing process to each tampered block.

7.2.2 Objectives of proposed work for color images

- To generate an authentication signal for each block of a red ,green and blue grayscale components of document image.
- To form authentication PNG image by combining the authentication signals computed from each block of a red ,green and blue grayscale components of document image.
- To form PNG image by combining the alpha channel plane with the original grayscale image.
- To embed authentication signal computed from the red grayscale component of document image into alpha channel of PNG image formed in the above step to yield a transparent stego-image with a disguise effect.
- To implement the image authentication process to mark image block as tampered or not.
- To implement data repairing process to each tampered block.

7.3 Methodology

7.3.1 System Architecture for grayscale images

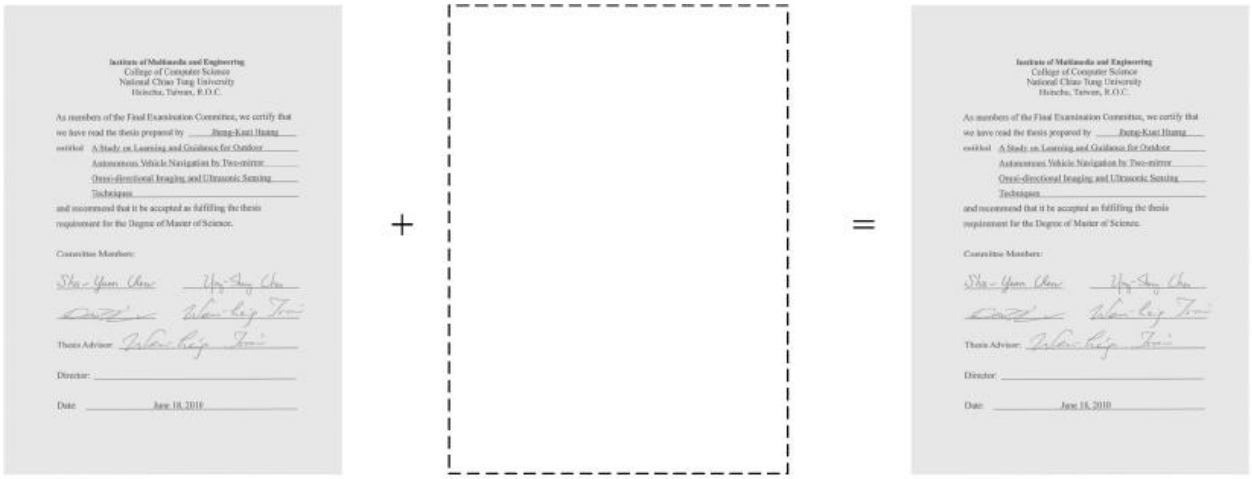


Figure 7.1: Illustration of creation of a PNG image from a grayscale document image and an additional alpha channel plane.

In the explored method, a PNG image is created from a binary-type grayscale document image with an alpha channel plane. The original image I may be thought as a grayscale channel plane of the PNG image. An illustration of this process of PNG image creation is shown in Fig.7.1. Next, it is binarized by moment-preserving thresholding [13], yielding a binary version of I , which we denote as I_b. Data for authentication and repairing are then computed from I_b and taken as input to the Shamir secret sharing scheme to generate secret shares. The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair capabilities. Two block diagrams describing the explored method are shown in Figs.7.2 and 7.3. Since the alpha channel plane is used for carrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication. In contrast, conventional image authentication methods often sacrifice part of image contents, such as least significant bits (LSBs) or flippable pixels,

to accommodate data used for authentication. In addition, once a stego-image generated from a conventional method such as an LSB-based one is unintentionally compressed by a lossy compression method, the stego-image might cause false positive alarms in the authentication system. In contrast, the explored method yields a stego-image in the PNG format, which, in normal cases, will not be further compressed, reducing the possibility of erroneous authentication caused by imposing undesired compression operations on the stego-image.

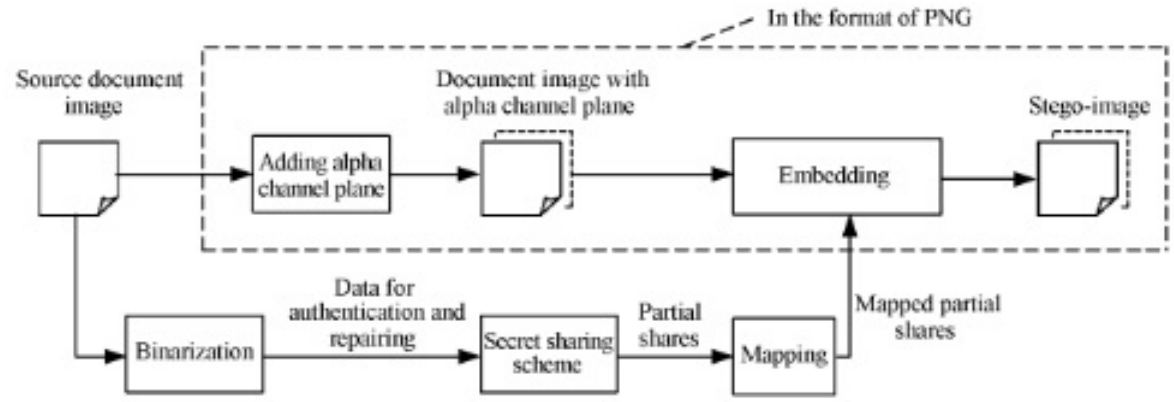


Figure 7.2: Creating a PNG image from a grayscale document image with an alpha channel.

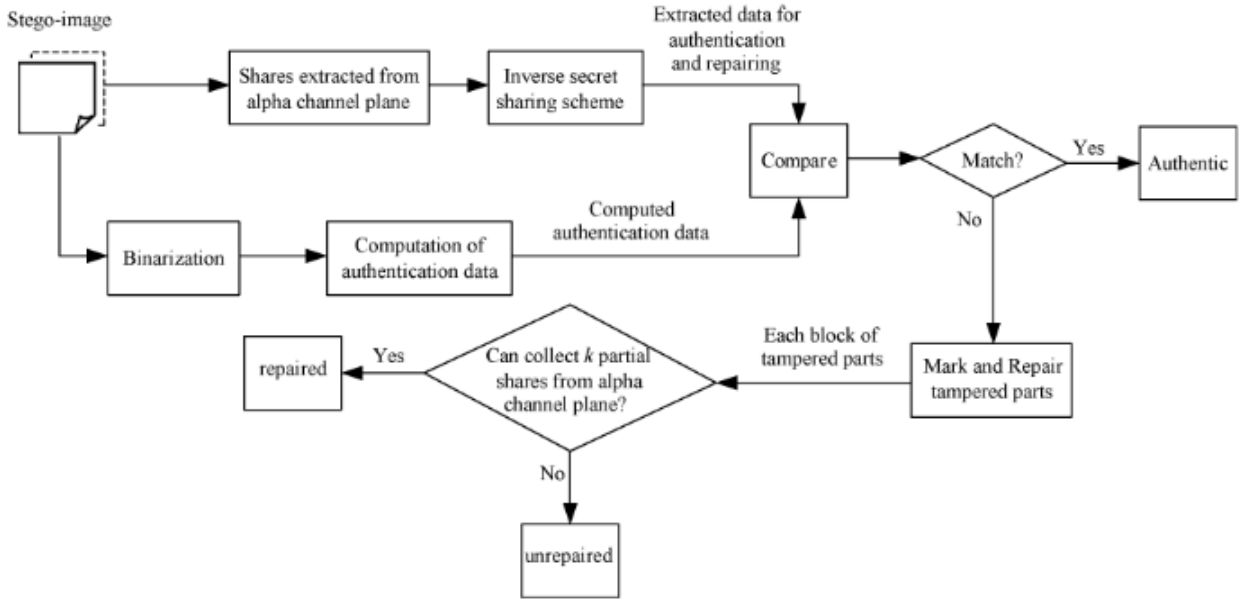


Figure 7.3: Authentication process including verification and self-repairing of a stego-image

7.3.2 System Architecture for color images

In the explored method, a PNG image is created from a color document image with an alpha channel plane. The original image I has three grayscale channel planes-red,green and blue. An illustration of this process of PNG image creation is shown in Fig.7.4. Next, each red,green and blue component is binarized by moment-preserving thresholding [13], yielding a binary version of I . Data for authentication and repairing are then computed from binary versions of red,green and blue components and taken as input to the Shamir secret sharing scheme to generate secret shares separately. The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares generated from red plane are randomly embedded into the alpha channel of original color image I for the purpose of promoting the security protection and data repair capabilities. Secrete shares generated from each of red,green and blue components of original color image I are embedded into red,green and blue components respectively of a new color image(an authentication color image).Five block diagrams describing the explored method are shown in Fig.7.4 -7.8. Since the alpha channel plane is used for carrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication.

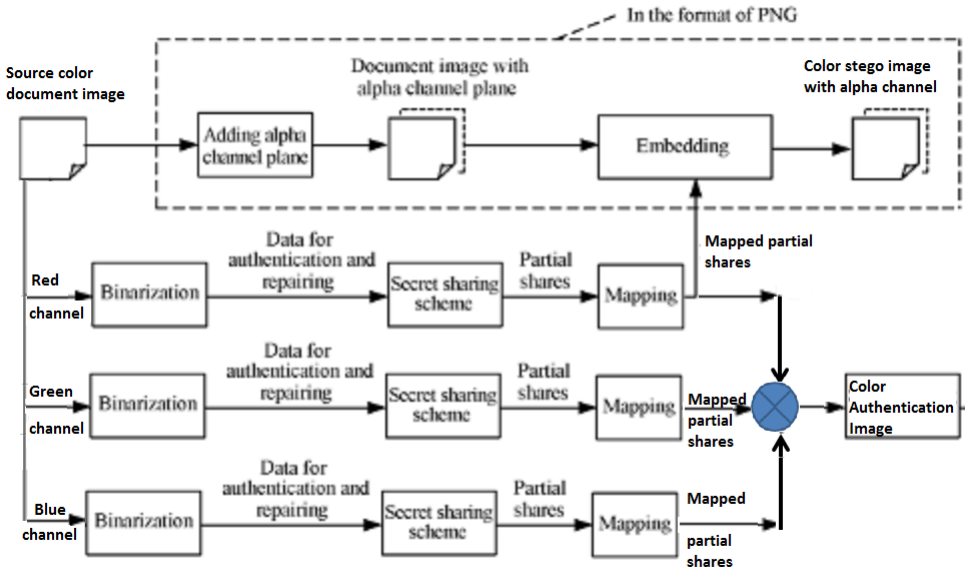


Figure 7.4: Creating a PNG image from a color document image with an alpha channel.

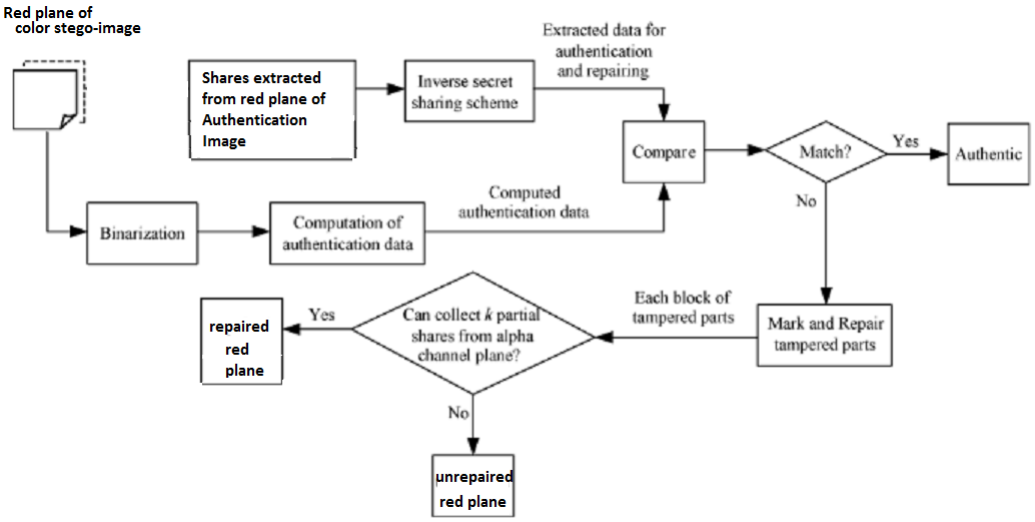


Figure 7.5: Authentication process including verification and self-repairing of a red component of color stego-image

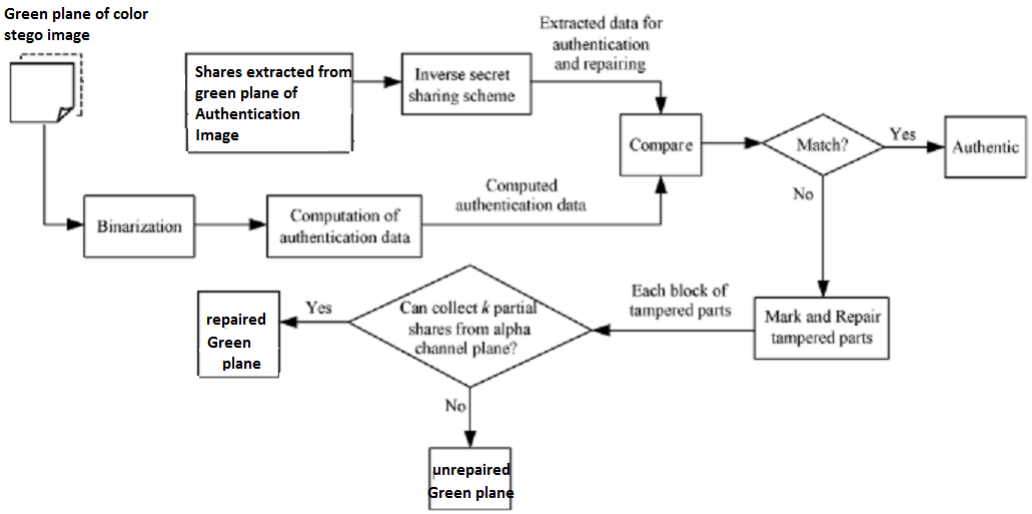


Figure 7.6: Authentication process including verification and self-repairing of a green component of color stego-image

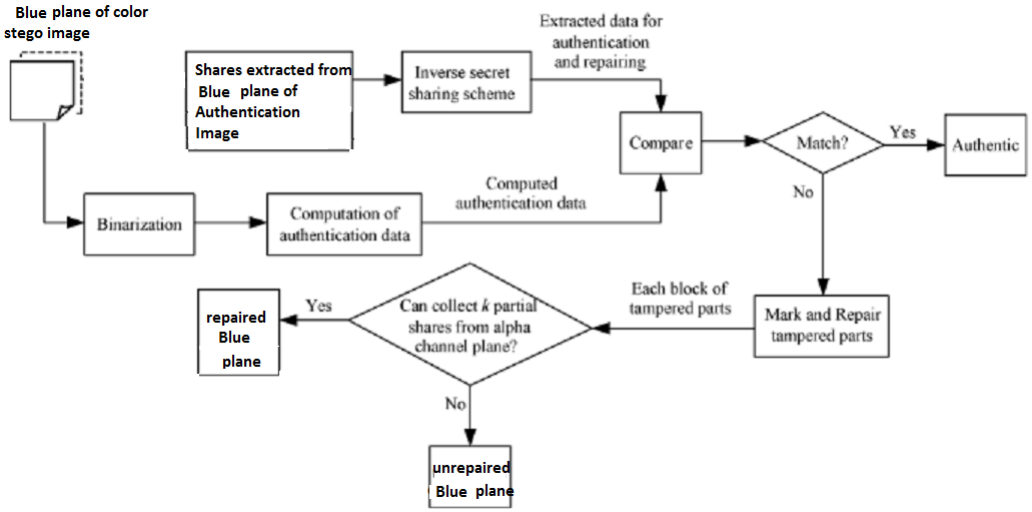


Figure 7.7: Authentication process including verification and self-repairing of a blue component of color stego-image

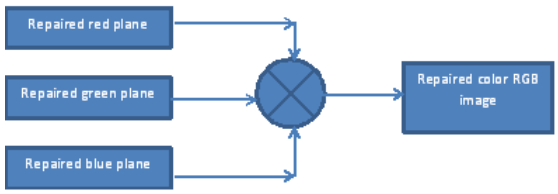


Figure 7.8: Recovery of color stego image from recovered red,green,and blue components

7.3.3 Modules

Module 1:(k, n)-threshold secret sharing

Input: secret d in the form of an integer, number n of shares, and threshold k < =n.

Output: n shares in the form of integers for the n participants to keep.

Algorithm: This module uses Shamir secret sharing scheme which allows the original secret message d to be divided in to n shares to be kept by n participants and as long as k of the n shares are availale the original secret message d can be recovered where k <= n.This method is called (k, n)-threshold secret sharing because minimum k shares out of n shares are required in order to recover orignal message d.

Step 1. Choose randomly a prime number p that is larger than d.

Step 2. Select k-1 integer values c_1,c_2,c_3,...,c_k within the range of 0 through p-1.

Step 3. Select n distinct real values x_1,x_2,x_3,...,x_n.

Step 4. Use the following k-1 degree polynomial to compute n function values F(x_i) , called partial shares for i=1,2,3,...,n. i.e.,

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + ...c_k - 1x_i^{k-1})_{modp} \tag{7.1}$$

Step 5. Deliver the two-tuple ($x_i, F(x_i)$as a share to the n th participant, where i=1,2,3...n.

Module 2: Secret recovery

Input: k shares collected from the participants and the prime number p with both k and p being those used in module 1.

Output: secret hidden in the shares and coefficients used in (1) in Algorithm 1, where i=1,2,3,..,k-1.

Algorithm: Since there are k coefficients, namely, d and $c_1, c_2, c_3, ..., c_{k-1}$ in (1) above, it is necessary to collect at least k shares from the n participants to form equations of the form of (1) to solve these coefficients in order to recover secret . This explains the term threshold for and the name (k,n)threshold for the Shamir method.

Steps:

1. Use the k shares $(x_1, F(x_1), (x_2, F(x_2), ..., (x_k, F(x_k)$ to set up

$$F(x_j) = (d + c_1 x_j + c_2 x_j^2 + ... + c_{k-1} x_j^{k-1})_m odp \tag{7.2}$$

   where j=1,2,3,...,k.

2. Solve the k equations above by Lagrange's interpolation to obtain d as follows [12]:

$$\begin{aligned} \text{d} = (-1)^{k-1}\{F(x_1)&\frac{x_2 x_3 ... x_k}{(x_1 - x_2)(x_1 - x_3)...(x_1 - x_k)} \\ &+ F(x_2)\frac{x_1 x_2 ... x_k}{(x_2 - x_1)(x_2 - x_3)...(x_2 - x_k)} + ... \\ &+ F(x_k)\frac{x_1 x_2 ... x_{k-1}}{(x_k - x_1)(x_k - x_3)...(x_k - x_{k-1})}\}\text{modp} \end{aligned} \tag{7.3}$$

$$\begin{aligned} \mathrm{F(x)} = \{\ F(x_1)\frac{(x-x_2)(x-x_3)...(x-x_k)}{(x_1-x_2)(x_1-x_3)...(x_1-x_k)} \\ + F(x_2)\frac{(x-x_1)(x-x_3)...(x-x_k)}{(x_2-x_1)(x_2-x_3)...(x_2-x_k)} + ... \\ + F(x_k)\frac{(x-x_1)(x-x_2)...(x-x_{k-1})}{(x_k-x_1)(x_k-x_3)...(x_k-x_{k-1})}\}\mathrm{modp} \end{aligned} \quad (7.4)$$

Module 3: Generation of a stego-image in the PNG format from a given grayscale image.

Input: a grayscale document image I with two major gray values and a secret key K.

Output: stego-image in the PNG format with relevant data embedded, including the authentication signals and the data used for repairing.

Algorithm:

Stage I:Generation of authentication signals.

In this stage input image binarization is performed by applying moment-preserving thresholding.Then the cover image I is transformed into the PNG format with an alpha channel plane I_α by creating a new image layer with 100 % opacity and no color as I_α .Then from each 2 x 3 block of image I generate 2 bit signals for authentication and repairing.

Steps:

1. Input image binarization:Apply moment-preserving thresholding [13] to image I to obtain two representative gray values g_1 and g_2, compute $T = (g_1 + g_2)/2$, and use T as a threshold to binarize I , yielding a binary version with "0" representing g_1 and "1" representing g_2.

2. Transforming the cover image into the PNG format:Transform I into a PNG image with an alpha channel plane I_α by creating a new image layer with 100% opacity and no color as I_α and combining it with I using an image processing software package.

3. (Beginning of looping) Take in an unprocessed of with pixels raster-scan order a 2x3 block B_b of I_b with pixels $p_1, p_2, ..., p_6$.

4. Creation of authentication signals: Generate a 2-bit authentication signal $s = a_a a_2$ with $a_1 = p_1 \oplus p_2 \oplus p_3$ and $a_2 = p_4 \oplus p_5 \oplus p_6$, where $\oplus$ denotes the exclusive-or operation.

Stage II: Creation and embedding of shares.

Data for authentication and repairing computed is taken as input to the Shamir secret sharing scheme to generate secret shares. The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair capabilities.

Steps:

5. Creation of data for secret sharing: Concatenate the 8 bits of a_1,a_2 , and p_1 through p_6 to form an 8-bit string, divide the string into two 4-bit segments, and transform the segments into two decimal numbers m_1 and m_2,respectively.

6. Partial share generation: Set p ,c_i , and x_i in (1) of Algorithm 1 to be the following values: 1)p=17(the smallest prime number larger than 15); 2)$d = m_1$ and $c_1 = m_2$; and 3)$x_1 = 1, x_2 = 2, ..., x_6 = 6$. Perform Algorithm 1 as a (2, 6)-threshold secret sharing scheme to generate six partial shares q_1 through q_6 using the following equations:

$$q_i = F(x_i) = (d + c_1 x_i)_{modp} \tag{7.5}$$

where $i = 1, 2, ..., 6$

7. Mapping of the partial shares: Add 238 to each of q_1 through q_6, resulting in the new values of q'_1 through q'_6, respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane I_α.

8. Embedding two partial shares in the current block: Take block B_α in I_α corresponding to B_b in I_b , select the first two pixels in B_α in the raster-scan order, and replace their values by q'_1 and q'_2, respectively (Fig.7.9).

9. Embedding remaining partial shares at random pixels: Use key K to select randomly four pixels in I_α but outside B_α, which are *unselected yet* in this step, and not the first two pixels of any block; in the raster-scan order, replace the four pixels' values by the remaining four partial shares q'_3 q'_6 through generated above, respectively (Fig.7.9).

10. (End of looping) If there exists any unprocessed block in I_b, then go to Step 3; otherwise, take the final I in the PNG format as the desired stego-image I'.

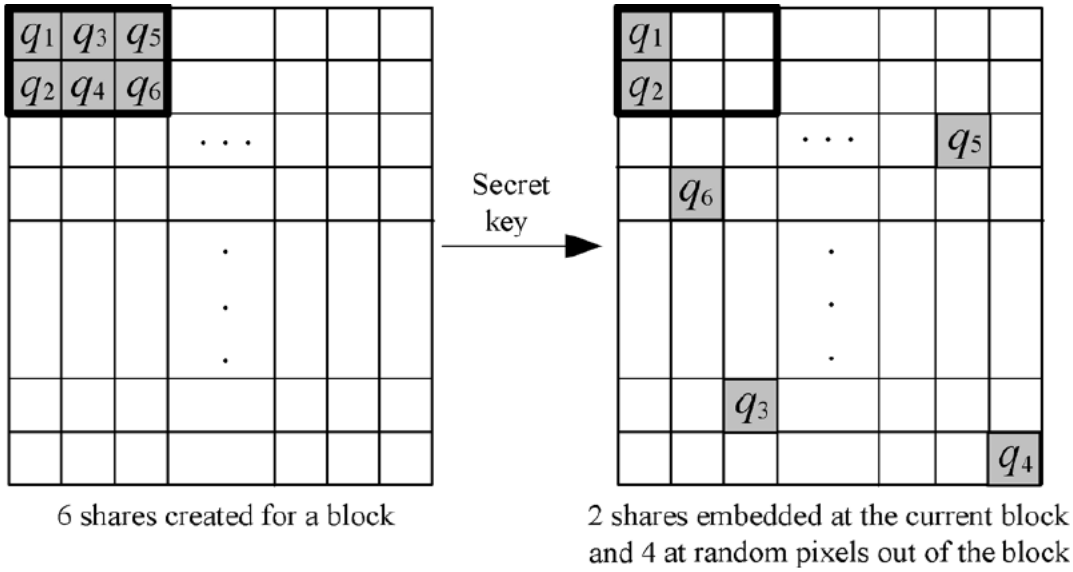


Figure 7.9: Illustration of embedding six shares created for a block: Two shares embedded at the current block, and the other four in four randomly selected pixels outside the block, with each selected pixel not being the first two ones in any block.

Comments:

The possible values of q_1 through q_1 yielded by (3) above are between 0 and 16 because the prime number p used there is 17. After performing Step 7 of the above algorithm, they become q_1' through q_6' , respectively, which all fall into a small interval of integers ranging from 238 to 254 with a width of 17 (the value of the prime number). The subsequent embedding of q_1' through q_6' in such a narrow interval into the alpha channel plane means that *very similar* values will appear everywhere in the plane, resulting in a *nearly uniform transparency* effect, which will not arouse notice from an attacker.

The reason why we choose the prime number to be 17 in the above algorithm is explained here. If it was instead chosen to be larger than 17, then the aforementioned interval will be enlarged, and the values of q_1' through q_6' will become possibly smaller than 238, creating an undesired *less transparent* but *visually whiter* stego-image. On the other hand, the 8 bits mentioned in Steps 5 and 6 above are transformed into two decimal m_1 and m_2 with their maximum values being 15 (see Step 5 above), which are constrained to lie in the range of 0 through p-1 (see Step 2 in Algorithm 1). Therefore,p should not be chosen to be smaller than 16. In short,$p = 17$ is an *optimal* choice.

As to the choice of the block size, the use of a larger block size, such as 2x4 or 3x3, will reduce the precision of the resulting integrity authentication (i.e., the stego-image will be verified in a spatially coarser manner). On the other hand, it seems that a smaller block size such as 2x2 instead of 2x3 may be tried to increase the authentication precision. However, a block in the alpha channel with a size of 2x2 can be used to embed only four partial shares instead of six (see Steps 6-9 of Algorithm 3). This decreases the share multiplicity and thus reduces the data repair capability of the method. In short, there is a tradeoff between the authentication precision and the data repair capability, and our choice of the block size of 2x3 is a balance in this aspect.

Module 4: Authentication of a given stego-image in the PNG format.

Input: stego-image I',the representative gray values g_1 and g_2, and the secret key K used in module 3.

Output: image I_r with tampered blocks marked and their data repaired if possible.

Algorithm: Authentication of a given stego-image in the PNG format.

Gray scale plane of given stego image is binarized and then authentication signals are computed from this binarized version and are compared with extracted data for authentication and repairing from alpha channel plane of given stego image.If match is found mark the block as authentic else mark block as a tampered and apply secret recovery algorithm from module 2 for data recovery.

Steps:

Stage I-extraction of the embedded two representative gray values.

1. Binarization of the stego-image: Compute $T = (g_1 + g_2)/2$, and use it as a threshold to binarize I' yielding a binary version I'_b of I' with "0" representing g_1 and "1" representing g_2.

   Stage II-verification of the stego-image.

2. (Beginning of looping) Take in a raster-scan order an unprocessed block B'_b from I'_b with pixel values p_1 through p_6, and find the six pixels' values q'_1 through q'_6 of the corresponding block B'_α in the alpha channel plane I'_α of I' .

3. Extraction of the hidden authentication signal:Perform the following steps to extract the hidden 2-bit authentication signal $s = a_1a_2$ from B'_α:

   (a) Subtract 238 from each of q'_1 and q'_2 to obtain two partial shares q'_1 and q'_2 of B'_b, respectively.

   (b) With shares $(1, q_1)$ and $(2, q_2)$ as input, perform Algorithm 2 to extract the two values d and c_1 (the secret and the first coefficient value, respectively) as output.

(c) Transform d and c_1 into two 4-bit binary values,concatenate them to form an 8-bit string S, and take the first 2 bits a_1 and a_2 of S to compose the hidden authentication signal $s = a_1a_2$.

4. Computation of the authentication signal from the current block content: Compute a 2-bit authentication signal $s' = a'_1a'_2$ from values p_1 through p_1 of the six pixels of B'_b by $a'_1 = p_1 \oplus p_2 \oplus p_3$ and $a'_2 = p_4 \oplus p_5 \oplus p_6$.

5. Matching of the hidden and computed authentication signals and marking of tampered blocks: Match s and s' by checking if $a_1 = a'_1$ and $a_2 = a'_2$, and if any mismatch occurs , mark B'_b,the corresponding block B' in I' and all the the partial shares embedded in B'_α as tampered.

6. (End of looping) If there exists any unprocessed block in I_b, then go to Step 2; otherwise, continue.

Stage III:-self-repairing of the original image content

7. Extraction of the remaining partial shares: For each block B'_α in I'_α, perform the following steps to extract the remaining four partial shares q_3 through q_6 of the corresponding block B'_b in I'_b from blocks in I'_α other than B'_α .

   (a) Use key K to collect the four pixels in I'_α in the same order as they were randomly selected for B'_b in Step 9 of Algorithm 3, and take out the respective data $q'_3, q'_4, q'_5,$ *and* q'_3 embedded in them.

   (b) Subtract 238 from each of q'_3 through q'_6, to obtain q_3 through q_6 respectively.

8. Repairing the tampered regions) For each block B' in I' marked as tampered previously, perform the following steps to repair it if possible.

   (a) From the six partial shares q_1 through q_6 of block B'_b in I'_b corresponding to B' (two computed in Step 3(1) and four in Step 7(2) above), choose two of them, e.g.,q_k and q_l , which are not marked as tampered, if possible.

   (b) With shares (k, q_k) and (l, q_l) as input, perform Algorithm 2 to extract the values of d and c_1(the secret and the first coefficient value, respectively) as output.

(c) Transform d and c_1 into two 4-bit binary values, and concatenate them to form an 8-bit string S'.

(d) Take the last 6 bits $b'_1, b'_2, ..., b'_6$, from S', and check their binary values to repair the corresponding tampered pixel values $y'_1, y'_2, ..., y'_6$, of block B' by the following way: if $b'_i = 0$, set $y'_i = g_1$; otherwise set $y'_i = g_2$ where $i = 1, 2, ..., 6$

9. Take the final I'as the desired self-repaired image I_r.

7.3.4 System Configuration

Hardware Requirement

- Processor - Pentium -IV
- Speed - 1.6 Ghz
- RAM - 1 GB
- Hard Disk - 160 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA.

Software Requirement

- Operating System -2000/XP/windows 7
- Front End - Java jdk 1.6 and above
- Tool - IDE Eclipse.

Chapter 8

Experimental Results and Comparision with Other Methods

8.1 Experimental Results Using a Document Image of a Scanned Check(Gray Image)

Experimental results yielded by the use of a document image of a check are shown in Fig.8.1, where the cover document image and the stego-image generated by the method are shown. Fig. 8.2 to Fig. 8.7 shows the result of authentication and data repairing under different types of attacks.The repaired pixels are shown in red. Also, we show the statistics of these experiment in Table 8.1 and Table 8.2.

The first results that we show here come from our experiments using a document image of a signed paper shown in Fig.8.1(left). The result of applying Algorithm 3 to embed share data into Fig. 8.1(first image) is shown in Fig. 8.1(second image). As shown, the stego-image shown in the latter is visually almost identical to the cover image shown in the former, although the alpha channel content of the latter image includes the embedded data.

We have also conducted image-modification attacks to the stego-images using two common image editing operations, namely, superimposing and painting. Tampered images yielded by the superimposing operation are presented in Figs.8.2-8.7. It can be observed from these

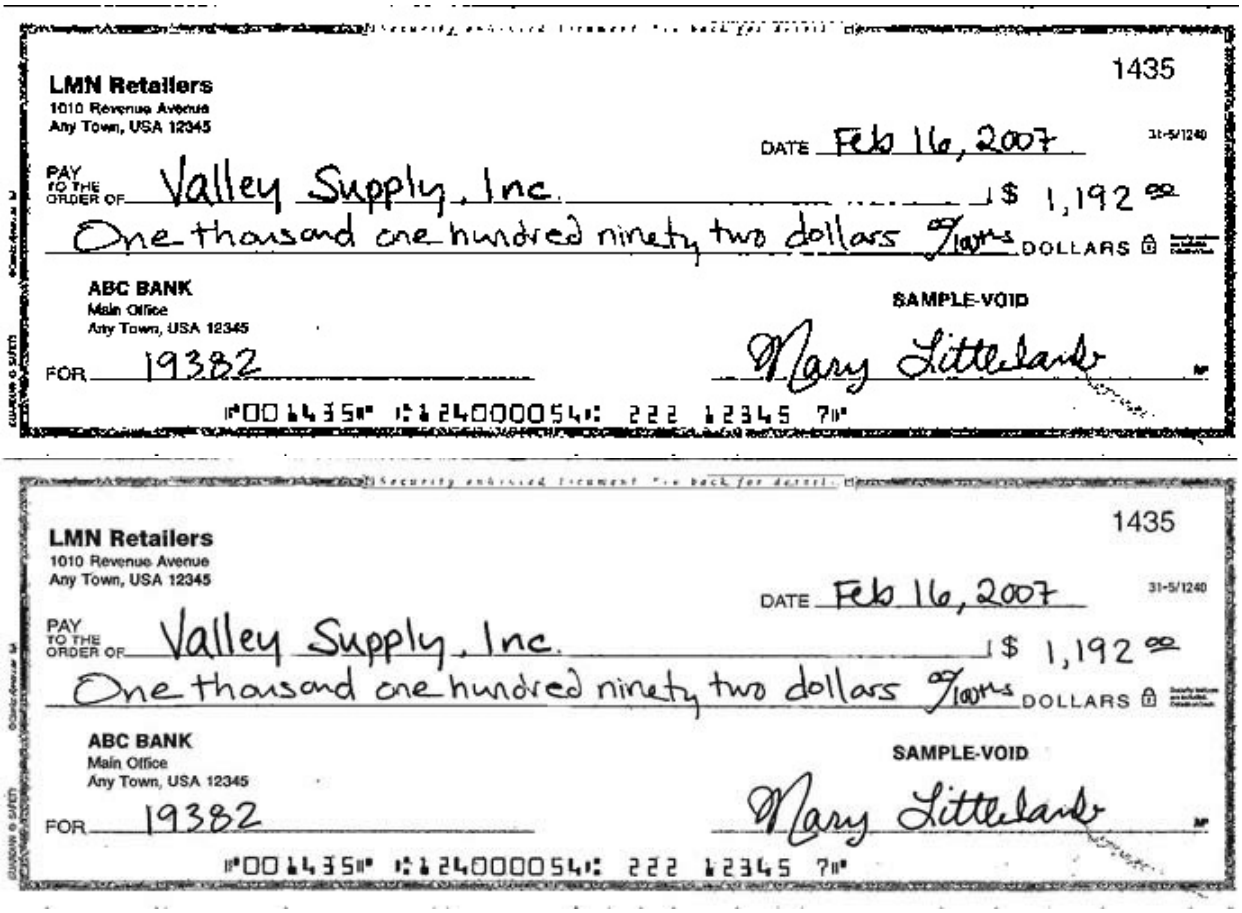


Figure 8.1: Experimental result of a document image of a signed paper. Original cover image(first image) and stego-image with embedded data(second image).

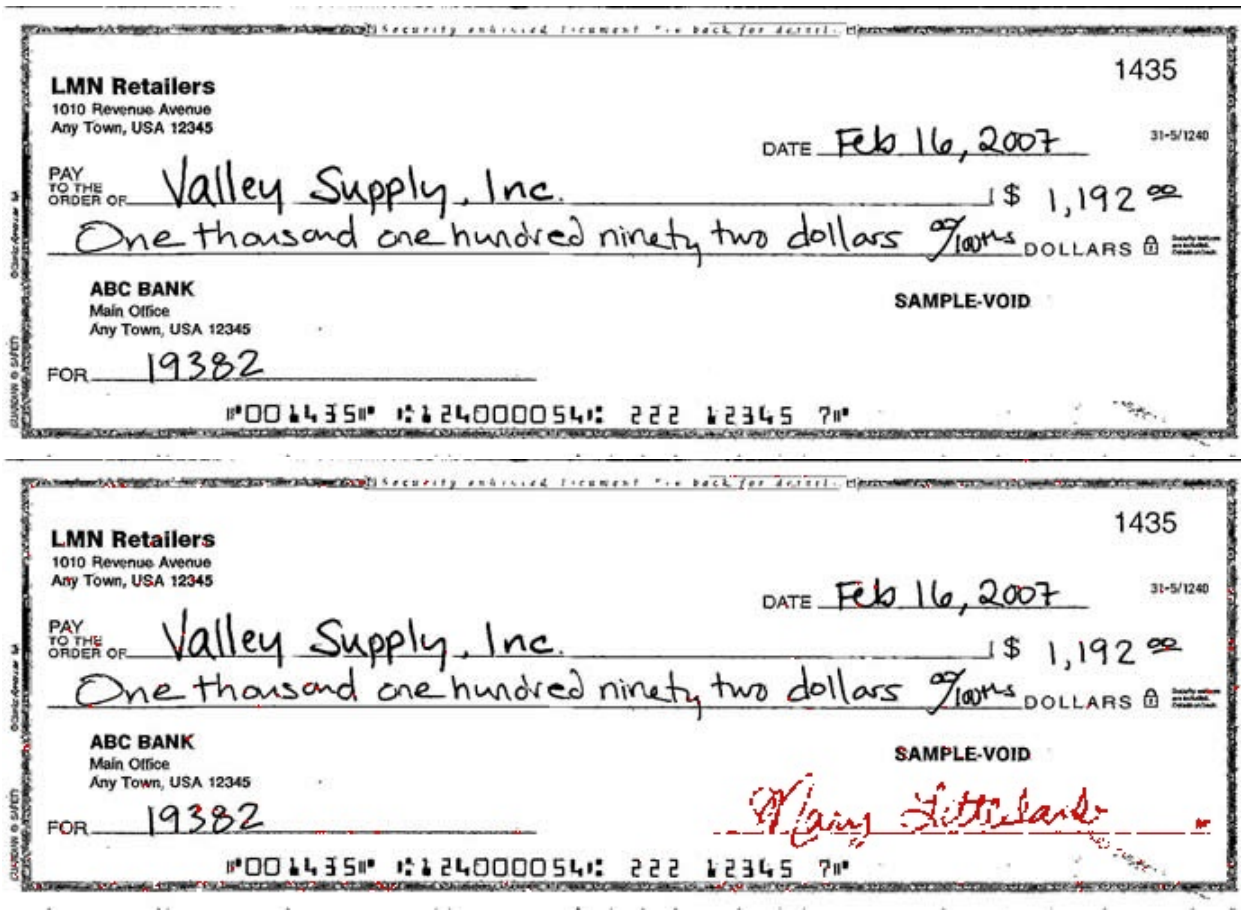


Figure 8.2: Authentication result of a document image of a signed paper attacked by superimposing a white rectangular shape on the signature. Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

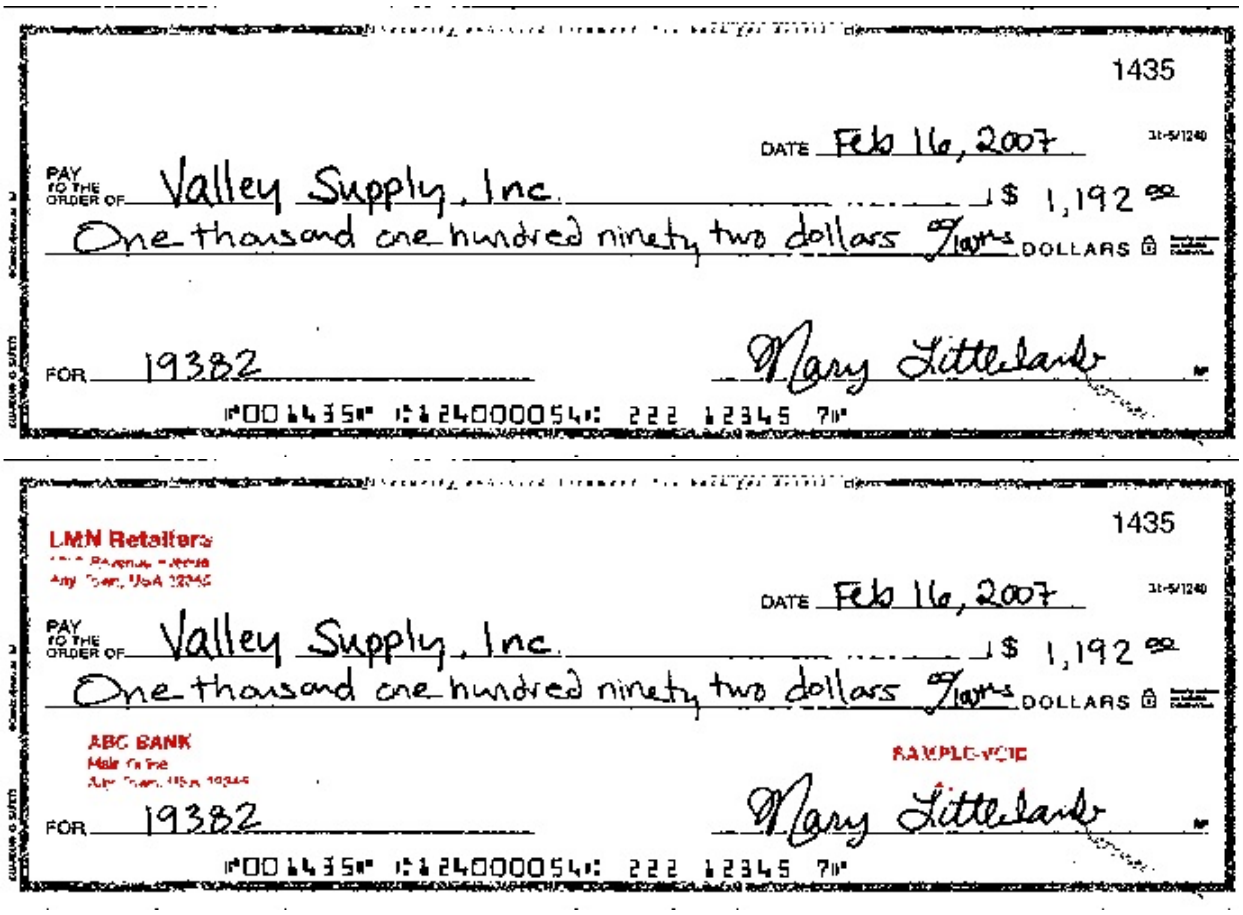


Figure 8.3: Authentication result of the document image of a signed paper attacked by superimposing a white rectangular shape on a piece of text. Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

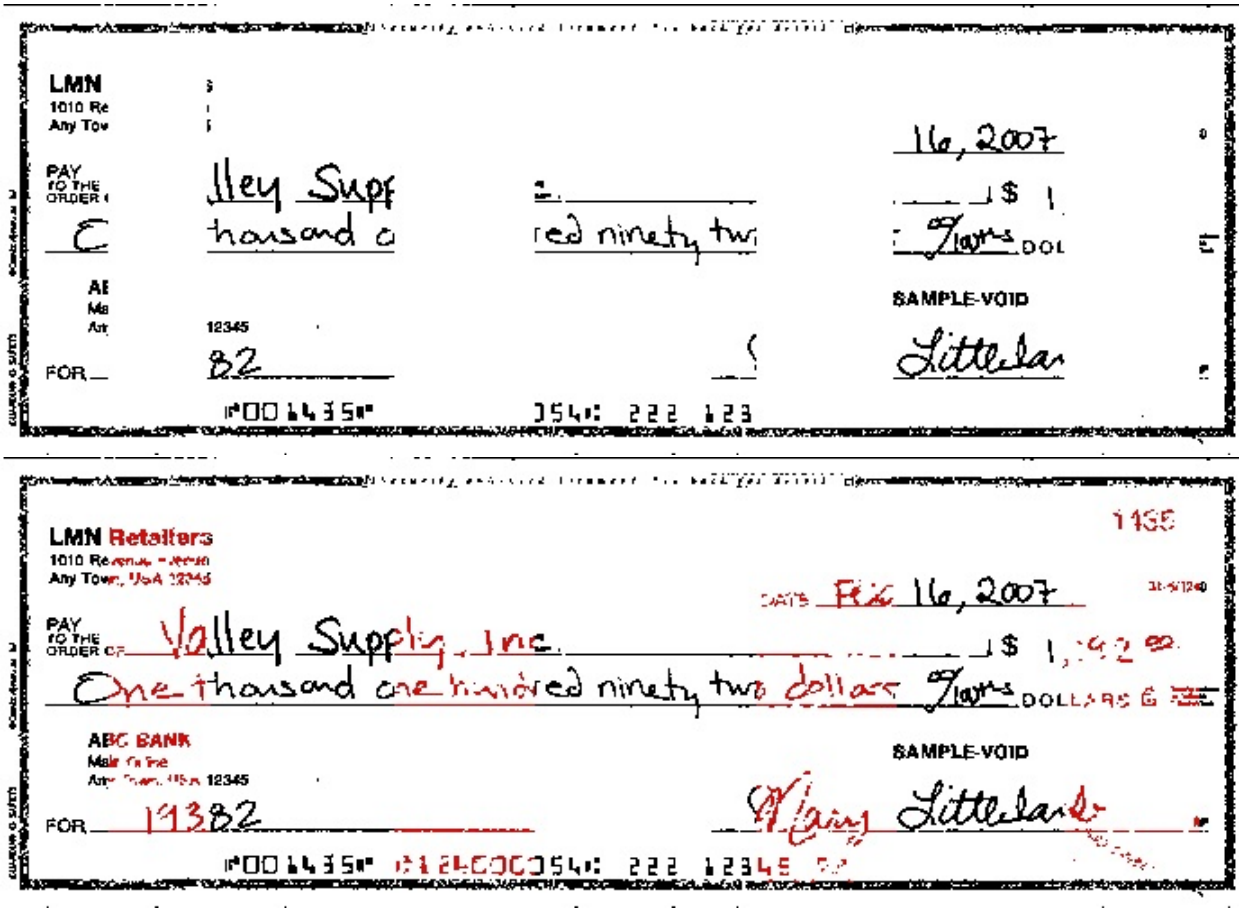


Figure 8.4: Authentication result of the document image of a signed paper attacked by superimposing white raster rectangular shapes on the content. Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

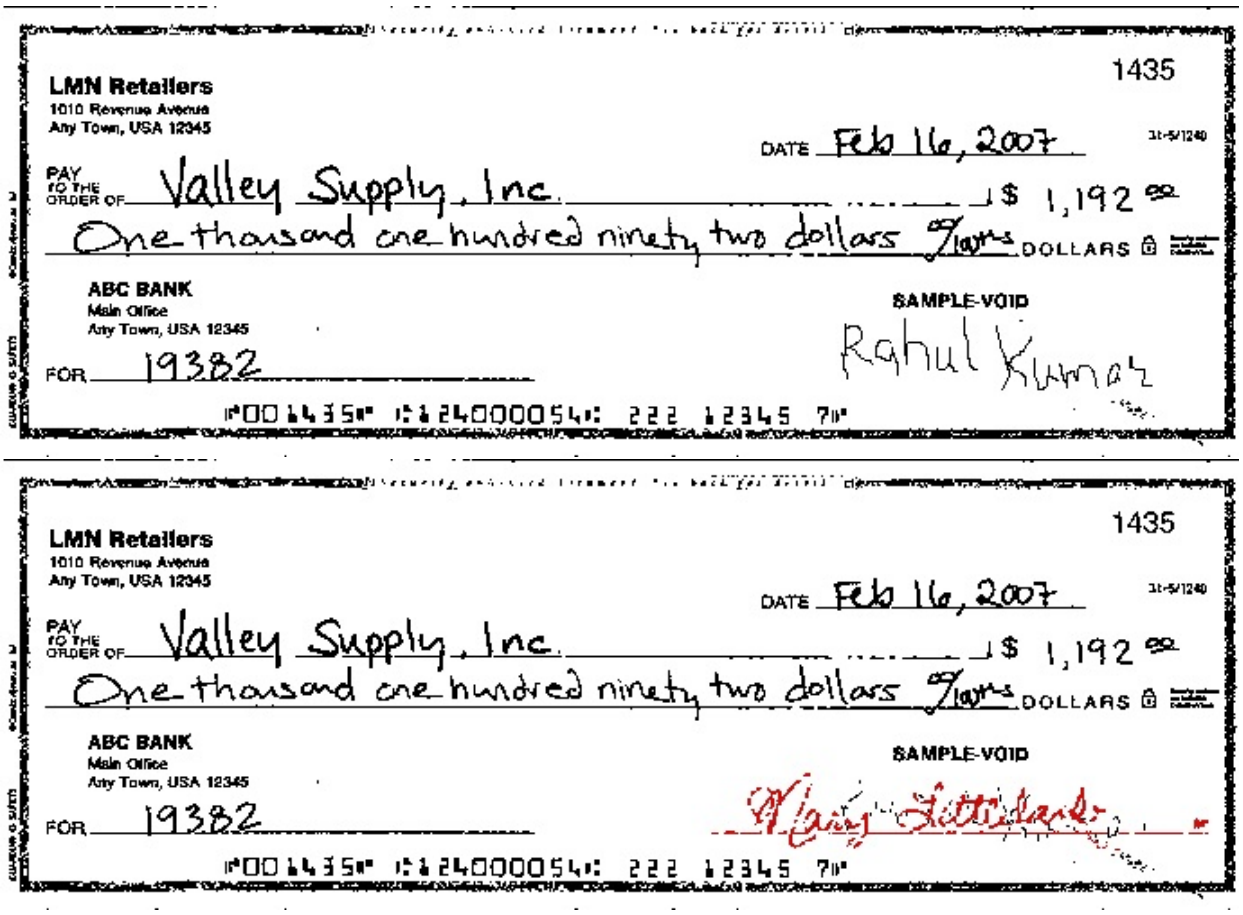


Figure 8.5: Authentication result of the document image of a signed paper attacked by painting white color on the original signature and texts and replacing the signature by a fake one. Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

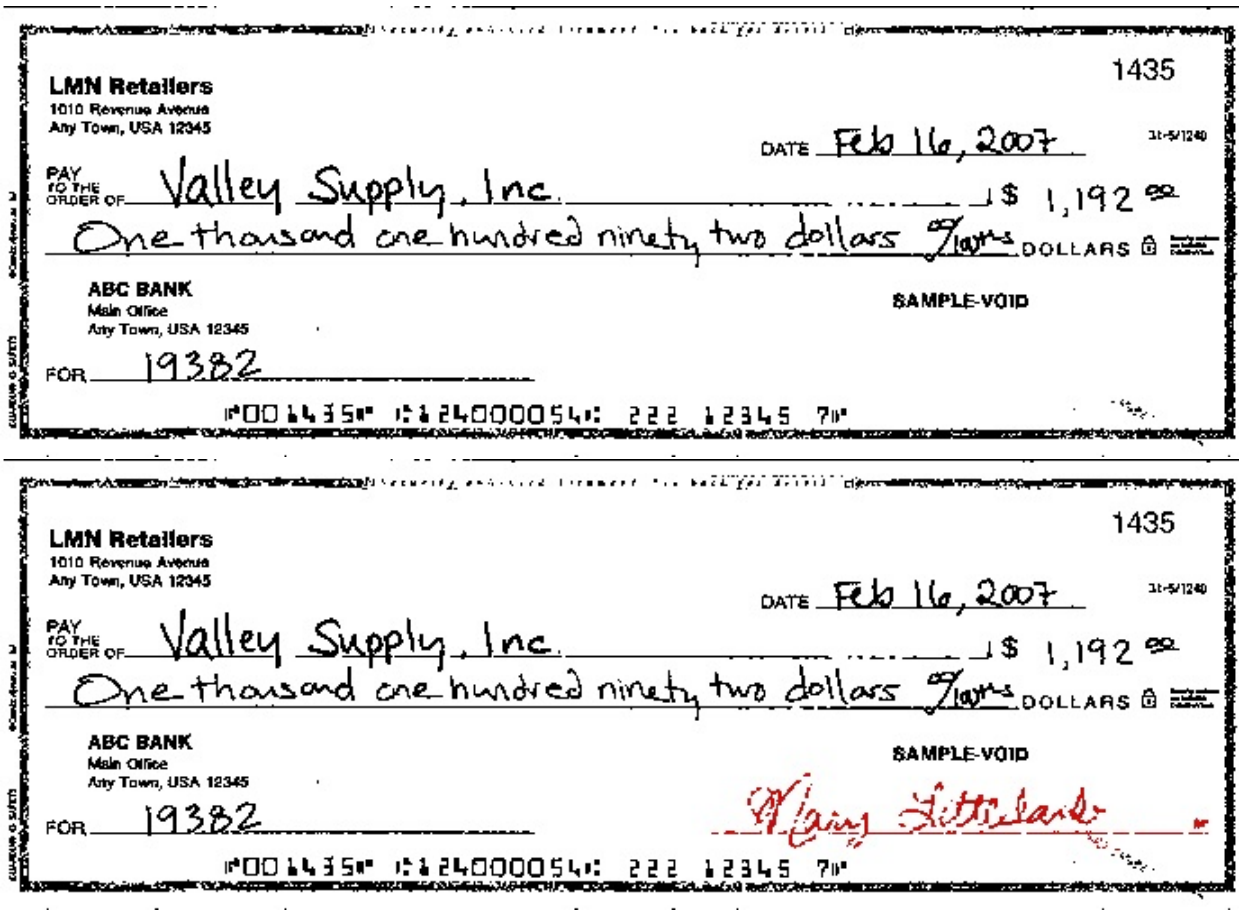


Figure 8.6: Authentication result of the document image of a signed paper attacked by painting white color on the original signature.Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

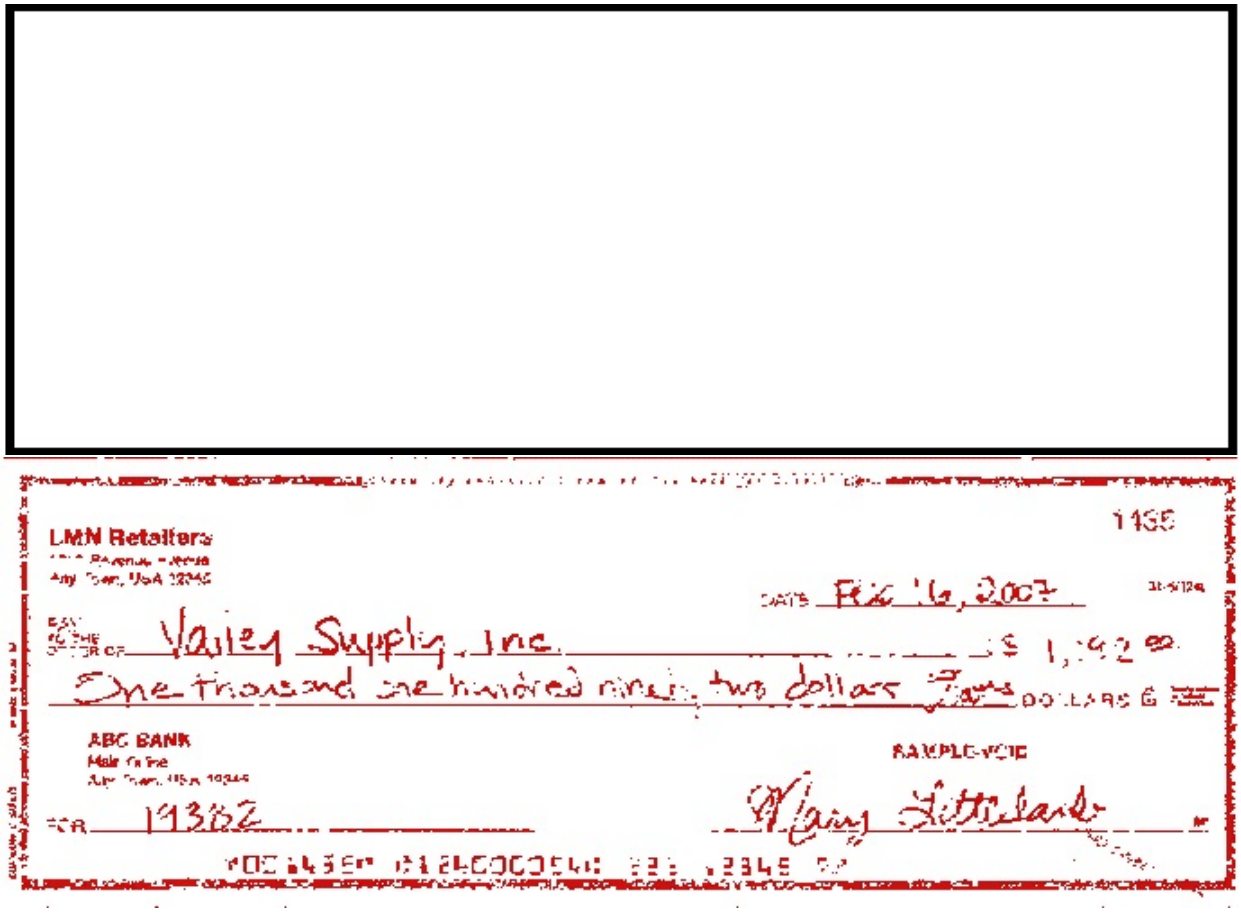


Figure 8.7: Authentication result of the document image of a signed paper attacked by painting white color on the entire content. Attacked stego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

experimental results that the superimposing operation, such as that provided by the image editing software Adobe Photoshop or Corel PhotoImpact, destroys the content of the alpha channel values by replacing all the original alpha channel values at the attacked part with the new values of 255. Since the largest alpha channel values created by the explored method is 254 (see Step 7 of Algorithm 3), all pixels with the unique values of 255 in the alpha channel plane may be easily detected as tampered by a modified version of Step 3 of Algorithm 4, which we describe as follows:

Step 3 (Checking of superimposing attacks and extraction of the hidden authentication signal) Check if both q_1' and q_2' are 255. If so, then regard the corresponding block B' in I' as attacked by superimposing, mark B' ,B_b' , and all the partial shares embedded in B_α' as tampered, and go to Step 6; otherwise, perform the original operations of Step 3 of Algorithm 4.

Fig. 8.5(first image) shows the result of superimposing a white rectan- gular shape with a fake signature "Rahul Kumar" on the genuine signa- ture "C. W. Lee" in the stego-image in Fig. 8.1((second image). Fig. 8.5(second image) shows the authentication result yielded by Algorithm 4. As shown, the superimposing rectangular part on the signature C. W. Lee has been completely detected. For each of the detected tampered blocks, if at least two untampered shares of it can be collected, its original content can be repaired, yielding the result shown in Fig. 8.5(second image).

In Fig. 8.5(first image), a text line under the signature in the signed paper disappeared after a white rectangular band was superim- posed on it. The results of image authentication and repairing are shown in Fig. 8.5(second image).

Table I includes the statistics of the performance of the pro- posed method shown by the above experimental results in terms of the five parameters, i.e., tampering, detection, repair, false- acceptance, and false-rejection ratios, which are defined in the following:

1. $tampering\ ratio = \dfrac{(the\ number\ of\ tampered\ blocks)}{(the\ \ total\ number\ of\ blocks)}$;

2. $detection\ ratio = \dfrac{(the number of detected blocks)}{(the\ number\ of\ tampered\ blocks)}$;
3. $repair\ ratio = (the\ number\ of\ repaired\ blocks)/(the\ number\ of\ detected\ blocks)$;
4. $false\ acceptance\ ratio = \dfrac{(the\ number\ of\ tampered\ blocks\ marked\ as\ untampered)}{(the\ total\ number\ of\ tampered\ blocks)}$;
5. $false\ rejection\ ratio = \dfrac{(the\ number\ of\ untampered\ blocks\ marked\ as\ tampered)}{(the\ total\ number\ of\ untamperedblocks)}$.

Note that the detection ratios are all 100% due to the ease in detection of the alpha channel values of 255 (using Step 3 described above) at image parts attacked by superimposing, as previously mentioned. Likewise, the alpha channel value corre- sponding to an intact block will not be 255 and can be easily checked to be so, yielding a false rejection rate of 0%. On the contrary, the alpha channel value corresponding to a tampered block is 255, which is easy to check as well, yielding a false ac- ceptance rate of 0%.

The content of a stego-image may be modified as well by the common operation of painting provided by well-known image editing software. Again, painting using Adobe Photoshop will replace the alpha channel values by 255, just like the superim- posing operation previously mentioned. However, it was found in this dissertation work that the painting operation provided by Corel PhotoImpact does not change the alpha channel values. There- fore, we conducted experiments of stego-image attacks using this type of painting. Some results are given in Figs. 8.5-8.7. In Fig.8.5, the painting operation was used to smear background gray values on the original signature "C.W.Lee" and write a fake signature "Rahul Kumar" on it, as shown in Fig.8.5(first image). Fig. 8.5(second image) shows the authentication result in which gray blocks were used again to indicate image parts where mismatching authentication signals were detected. Note that the smeared part (the signature C. W. Lee) and the added part (the signature "Rahul Kumar") have been both revealed by the authentication process. In addition, it can be seen that some black parts exist within the gray region, meaning that these parts, although tampered, were not detected by the explored method. This is due to the fact that there is actually a probability of 1/4 for an erroneous block authentication to occur because only two bits are created as the signal for block authentication (see Step 8 of

Table 8.1: STATISTICS OF EXPERIMENTAL RESULTS OF ATTACKS USING SUPERIMPOSING

Expt. Result	No. of blocks	No. of tampered blocks	No. of detected blocks	No. of repaired blocks	false acceptance ratio	false rejection ratio
Expt. shown in Fig.8.2	28666	23104	23104	23104	0%	0%
Expt. shown in Fig.8.3	28666	1525	1525	1525	0%	0%
Expt. shown in Fig.8.4	28666	7088	7088	7088	0%	0%

Algorithm 3 or Step 5 of Algorithm 4).

In Fig. 8.6(first image), the signature was removed by replacing it with the background gray value using painting. The results of image authentication and data repairing are shown in Figs.8.6(second image). Fig.8.7(first image) shows the results of removing the entire image content by painting. In both cases, the untouched content of the alpha channel values still yields repair results with their contents recognizable to a certain degree.

It is noted here that, when a stego-image is tampered with by painting, which does not change the content of the alpha channel plane, the hidden authentication signals and data for re- pairing are not destroyed. Therefore, the computed authentica- tion signals from the alpha channel values are always true, and as long as the computed authentication signal is not identical to the extracted authentication signal for a block, the block will be marked as having been tampered with. This explains why the false rejection rate is 0%. However, as previously mentioned, there is a probability of 1/4 for an erroneous block authentica- tion to occur because only 2 bits are created as the signal for block authentication, and this leads to a false acceptance ratio of at most 25%. These reasonings are verified by the performance statistics of Figs.8.5-8.7 listed in Table 8.2.

Table 8.2: STATISTICS OF EXPERIMENTAL RESULTS OF ATTACKS USING PAINTING OPERATIONS

Expt. Result	No. of blocks	No. of tampered blocks	No. of detected blocks	No. of repaired blocks	false acceptance ratio	false rejection ratio
Expt. shown in Fig.8.5	28666	2116	2116	2116	0 %	0%
Expt. shown in Fig.8.6	28666	1735	1735	1735	0 %	0%
Expt. shown in Fig.8.7	28666	20460	20460	20460	0%	0%

8.2 Experimental Results Using a Document Image of a Scanned Certificate(Color Image)

Experimental Results Using a Document Image of a Scanned Certificate(Color Image) are shown in Fig.8.8, where the cover document image and the stego-image generated by the method are shown. Fig. 8.9 to Fig. 8.16 shows the result of authentication and data repairing under different types of attacks.

8.3 Experimental Results Using a Image Database

Experimental results yielded by the use of a image database of 20 images comprising of various types of documents is summarized in the Fig.8.17-8.19.

8.4 Comparison of Performances with Other Methods

A comparison of the capabilities of the explored method with those of four existing methods is shown in Table 8.3. All but the explored method will create distortion in the stego-image during the authentication process. More importantly, only the explored method has the capability of repairing the tampered parts of an authenticated image.

Furthermore, among the methods with tampering localization capabilities at the block

Figure 8.8: Experimental result of a document image of a scanned certificate. Original cover image(first image) and stego-image with embedded data(second image).

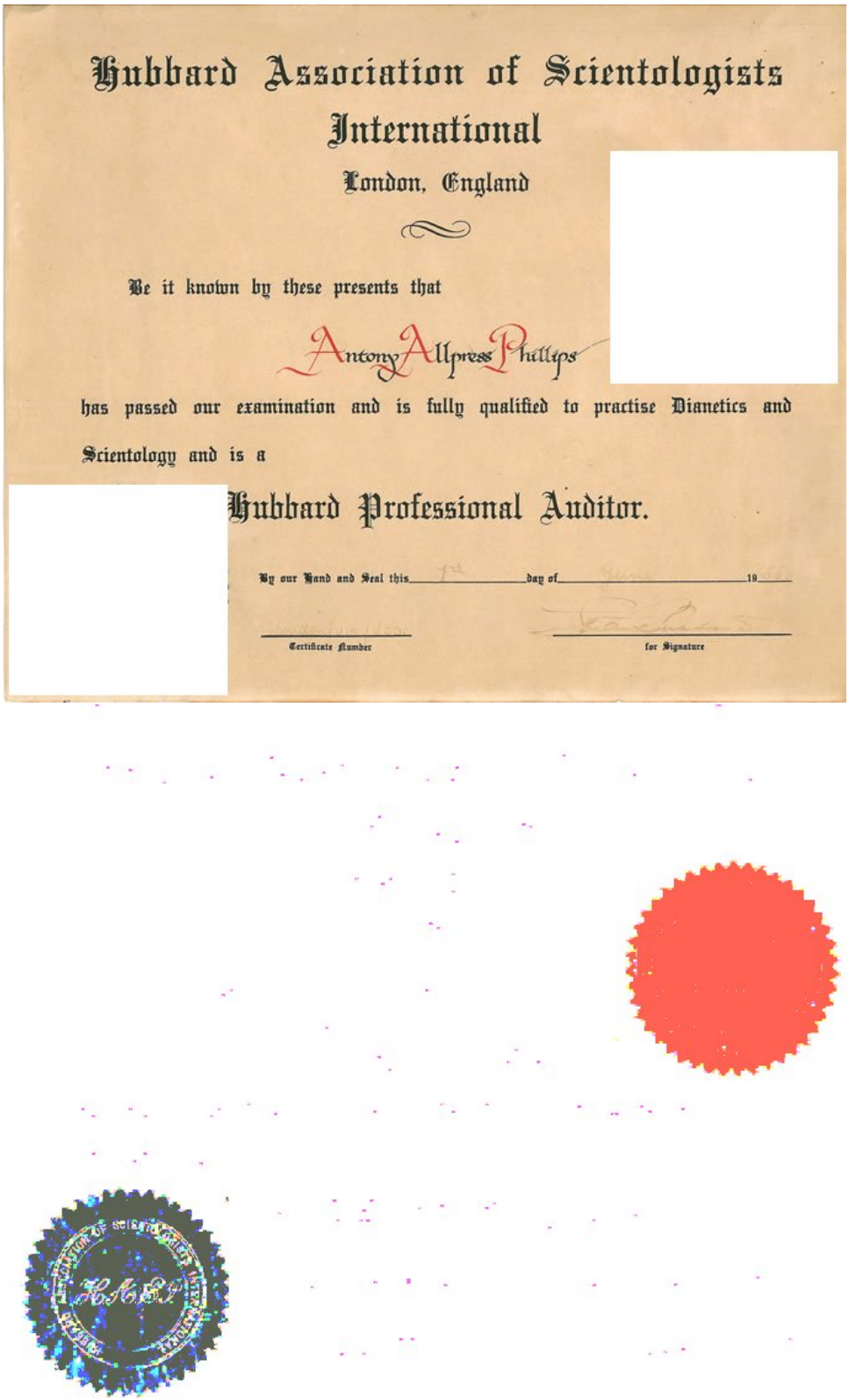


Figure 8.9: Authentication result of the document image of a scanned certificate attacked by superimposing white rectangular shapes on color logos. Attacked stego image(first image) and repaired stego-image (second image).

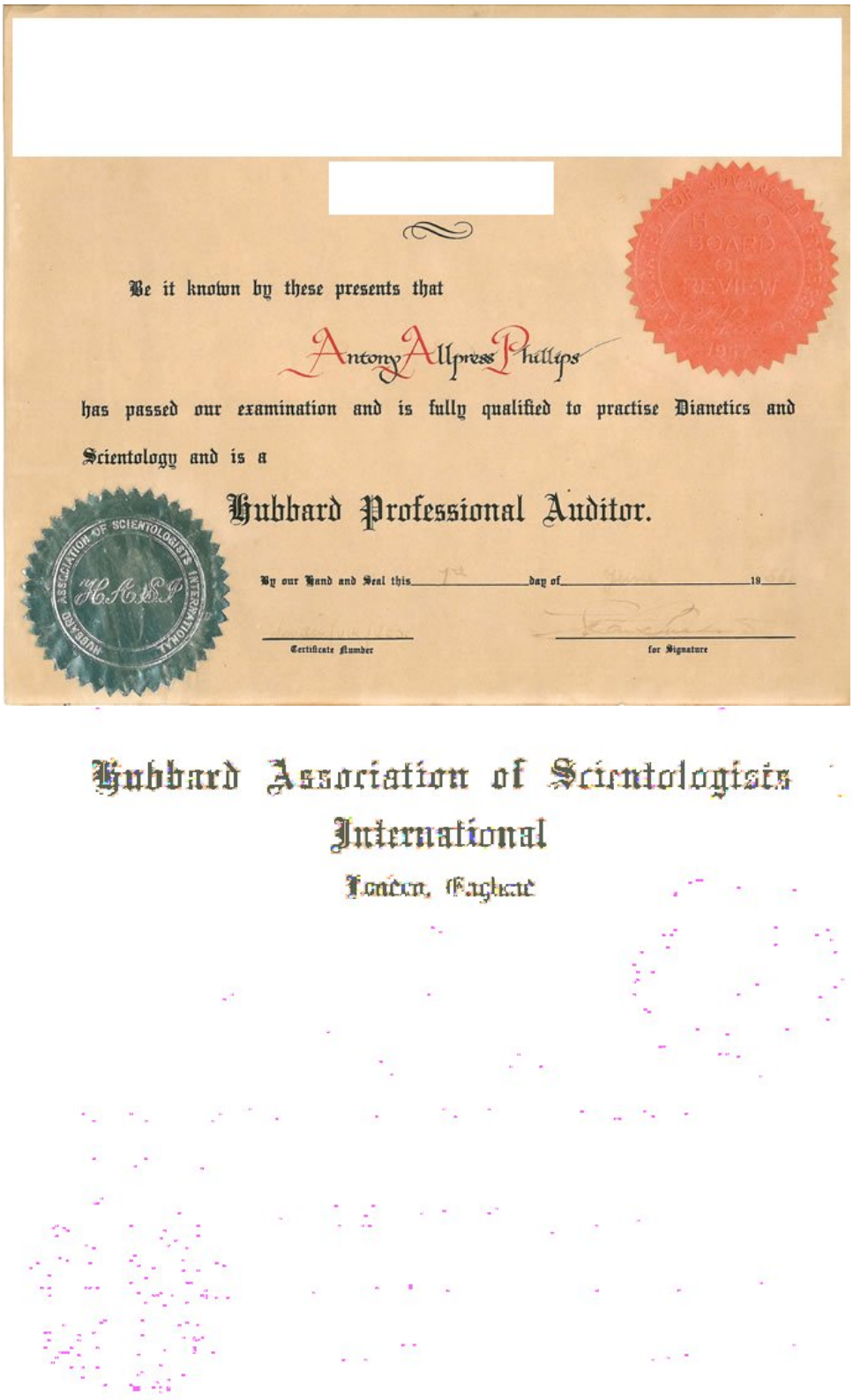


Figure 8.10: Authentication result of a document image of a scanned certificate attacked by superimposing white rectangular shapes on a piece of text . Attacked stego image(first image) and repaired stego-image(second image).

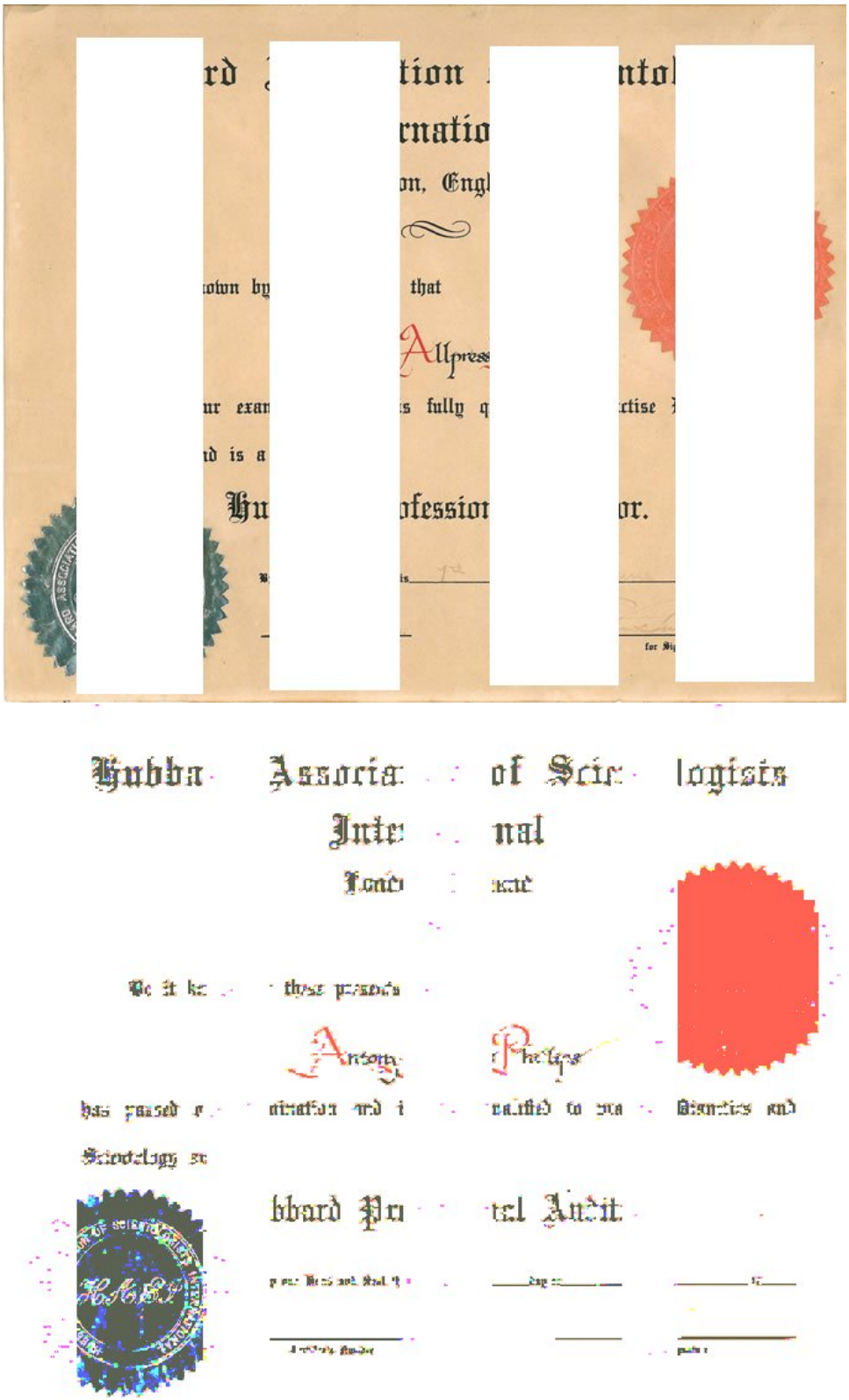


Figure 8.11: Authentication result of the document image of a scanned certificate attacked by superimposing white raster rectangular shapes on the content. Attacked stego image(first image) and repaired stego-image(second image).

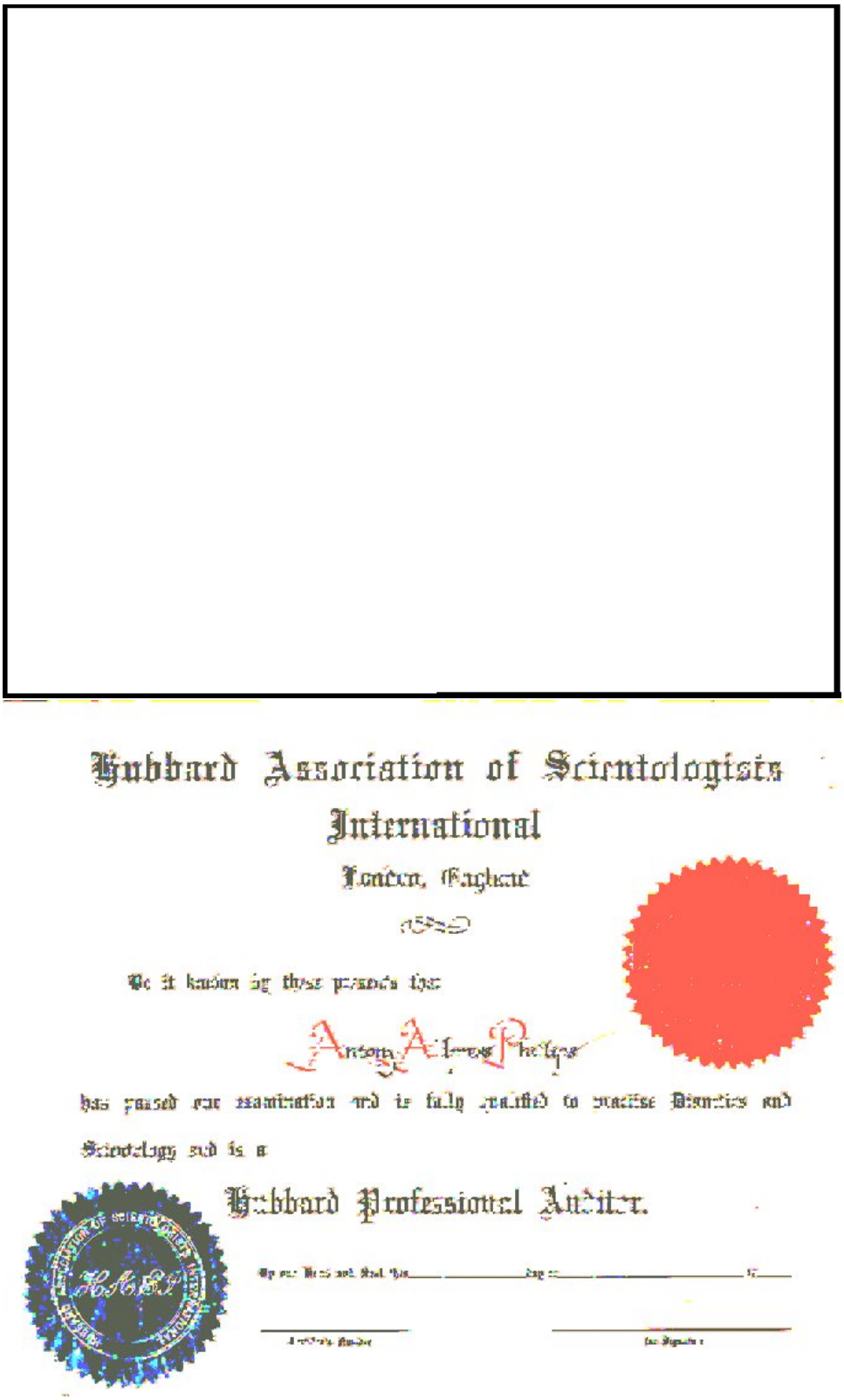


Figure 8.12: Authentication result of the document image of a scanned certificater attacked by painting white color on the entire content. Attacked stego image(first image) and repaired stego-image (second image).

Figure 8.13: Authentication result of the document image of a scanned certificate attacked by removing background. Attacked stego image(first image) and repaired stego-image (second image).

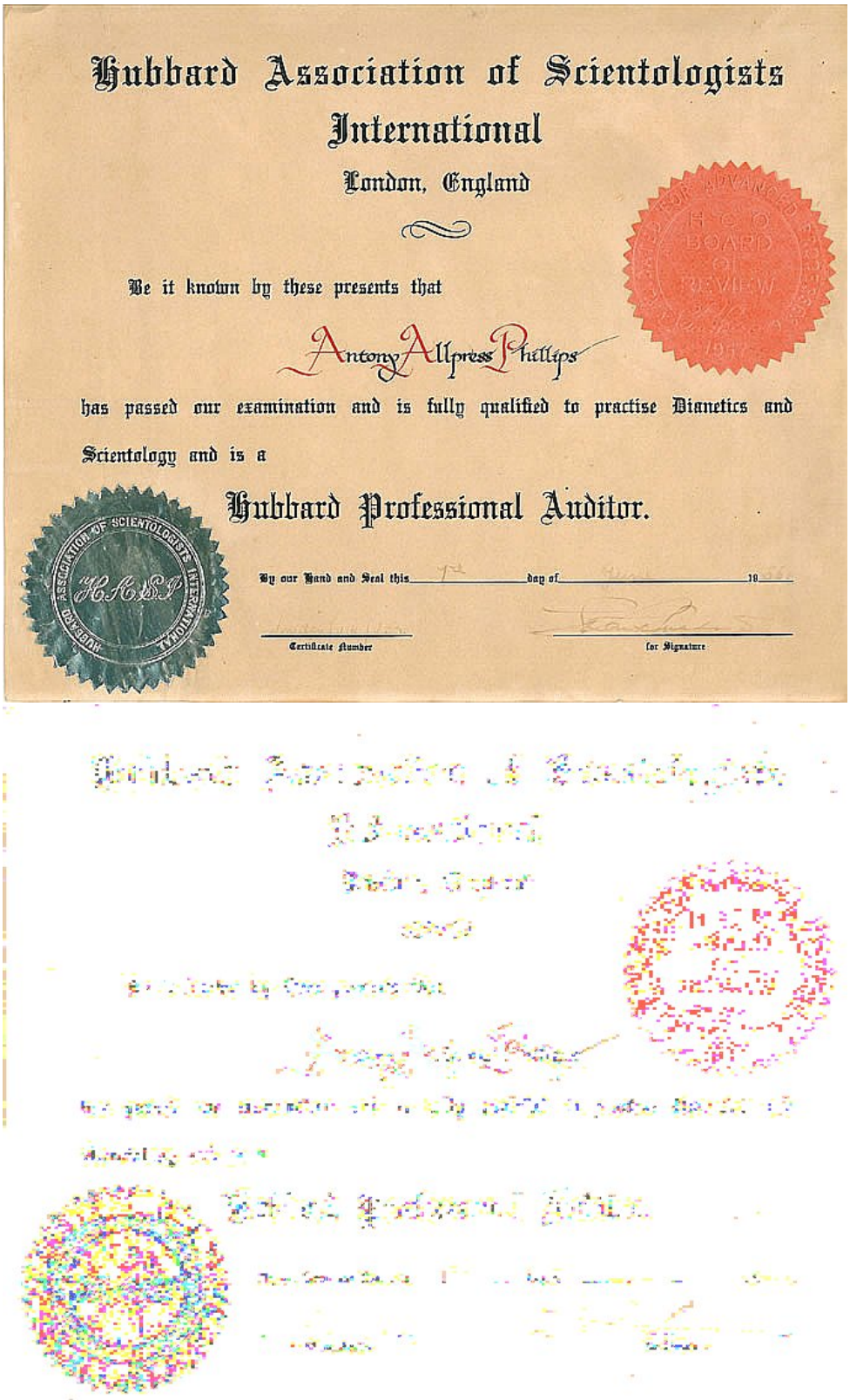


Figure 8.14: Authentication result of the document image of a scanned certificate attacked by sharpening. Attacked stego image(first image) and repaired stego-image (second image).

Figure 8.15: Authentication result of the document image of a scanned certificate attacked by smoothing. Attacked stego image(first image) and repaired stego-image (second image).

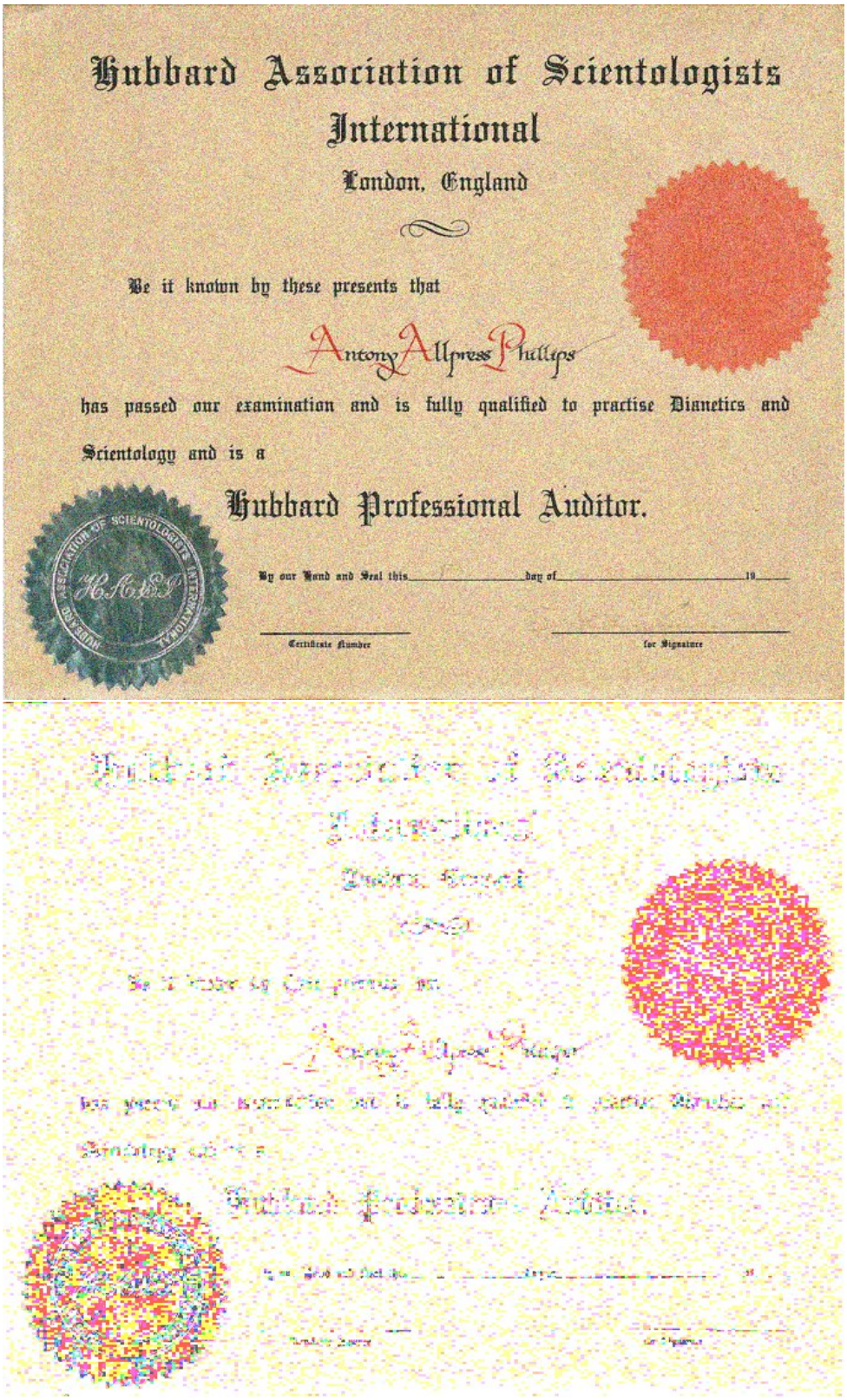


Figure 8.16: Authentication result of the document image of a scanned certificate attacked by changing standard deviation of color contents. Attacked stego image(first image) and repaired stego-image (second image).

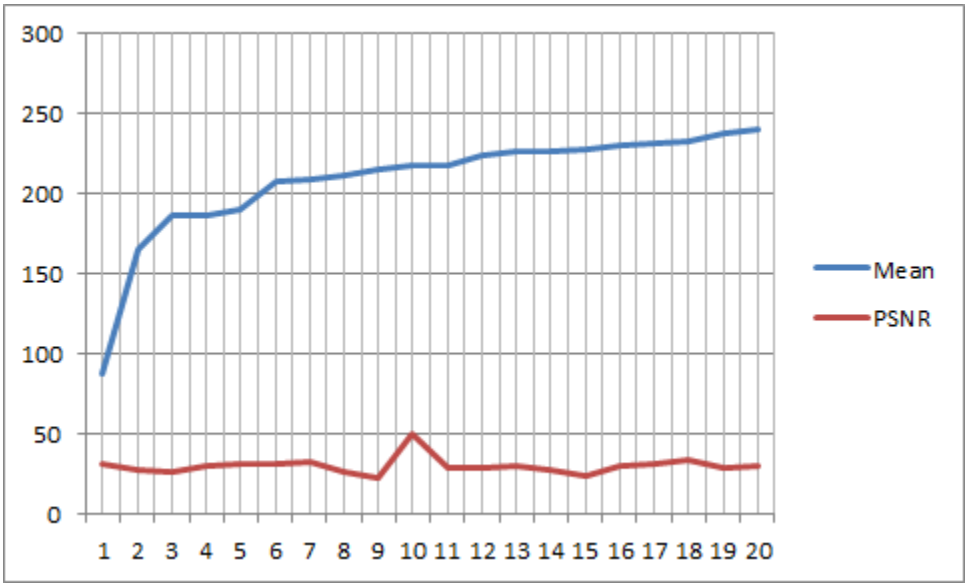


Figure 8.17: Mean (in ascending order) of cover images vs PSNR between cover and stego images

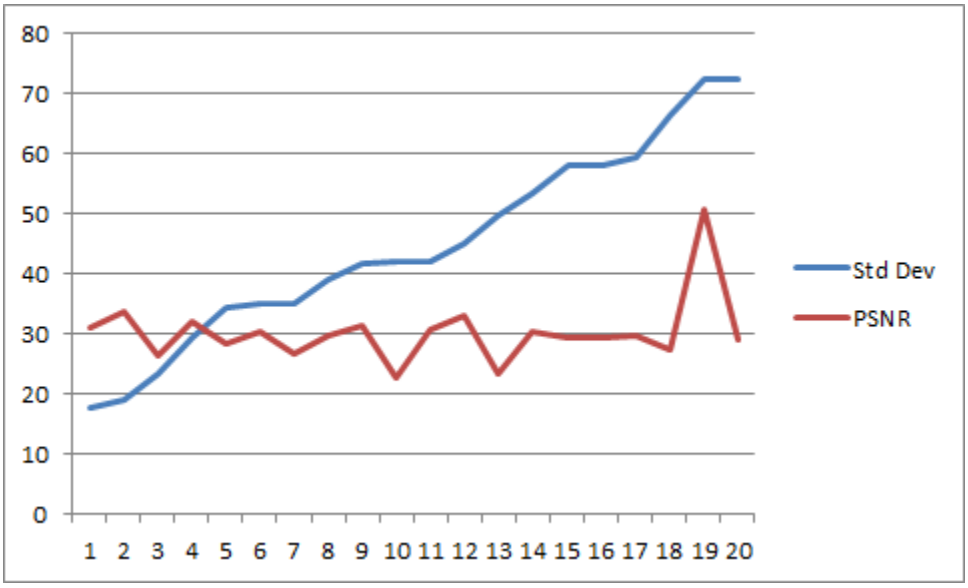


Figure 8.18: Standard deviation (in ascending order) of cover images vs PSNR between cover and stego images

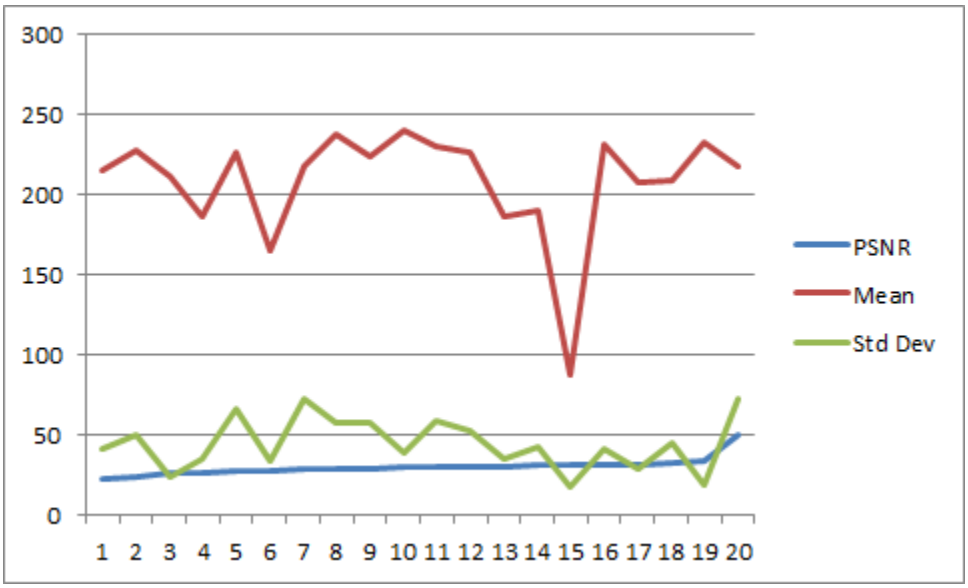


Figure 8.19: PSNR between cover and stego images(in ascending order) vs standard deviation and mean of cover images

Table 8.3: COMPARISON OF DOCUMENT IMAGE AUTHENTICATION METHODS

	Disto rtion in stego image	Tampe-ring local ization capabi-lity	Repair capability	Authent-ication Precis-ion	Distri-bution of Authen-ticated image parts	Manipu-lation of data embe-dding
Wu & Liu[4]	YES	NO	NO	Macro-block	Non-Blank Part	Pixel flippa-bility
Young & Kot[5]	YES	YES	NO	33 X 33 Block	Non-Blank Part	Pixel flippa-bility
Young & Kot[6]	YES	NO	NO	Macro-block	Non-Blank Part	Pixel flippa-bility
Tzeng & Tsai[7]	YES	YES	NO	64 X 64 Block	Entire-Image	Pixel Re-placement
Proposed method by Che-Wei Lee & Wen-Hsiang Tsai[1]	NO	YES	YES	2 X 3 Block	Entire-Image	Alpha chan-nel Pixel Replace-ment

level such as [5], [8], and the explored method, the explored method provides a finer authentication precision with the block size of 2x3. Specifically, the method in [5] needs larger macroblocks to yield pixel flippabilities for embedding authentication data. In the case of using smaller blocks, Tzeng and Tsai's method [8] has a high possibility to generate noise pixels, as mentioned in [6], and thus,they conducted experimental results with the larger block size of 64x64.

As to the distribution of authenticated image parts, because there exists no flippable pixel for use by the methods of [4]-[6] to embed data in all-white regions (such as marginal regions) of a document image, the distribution of authenticated image parts tends to be restricted to be on lines or strokes in the document, whereas the explored method does not have this limitation. Nevertheless, in [4]-[6], the authenticity of an image part including such all white regions can be still ensured by the use of cryptographic signatures embedded in other regions of the image. At last, the methods of [4]-[6] manipulate pixel flippability, and the method of [8] enforces pixel replacement for the aim of data embedding. The explored method is the only one that makes use of the alpha channel plane instead of the bit plane.

Chapter 9

Discussion

9.1 Merits of the Explored Method

In addition to being capable of data repairing and being blind in nature (requiring no overhead other than the stego-image), the explored method has several other merits, which are described in the following.

1. **Providing pixel-level repairs of tampered image parts:-**As long as two untampered partial shares can be collected, a tampered block can be repaired at the pixel level by the explored method. This yields a better repair effect for texts in images because text characters or letters are smaller in size with many curved strokes and need finer pixel-level repairs when tampered with.

2. **Having higher possibility to survive image content attacks:-**By skillfully combining the Shamir scheme, the authentication signal generation, and the random embedding of multiple shares, the explored method can survive malicious attacks of common content modifications, such as superimposition, painting, etc., as will be demonstrated by experimental results subsequently described.

3. **Making use of a new type of image channel for data hiding:-**Different from common types of images, a PNG image has the extra alpha channel plane that is normally used to produce transparency to the image. It is differently utilized by the explored method for the first time as a carrier with a large space for hiding share data.

As a comparison, many other methods use LSBs as the carriers of hidden data.

4. **Causing no distortion to the input image:-**Conventional image authentication methods that usually embed authentication signals into the cover image itself will unavoidably cause destruction to the image content to a certain extent. Different from such methods, the explored method utilizes the pixels' values of the alpha channel for the purpose of image authentication and data repairing, leaving the orig inal image (i.e., the grayscale channel) untouched and thus causing no distortion to it. The alpha channel plane may be removed after the authentication process to get the original image. Fig. 9.1 shows the framework of the explored method in this aspect, and Fig. 9.2, shown for comparison, illustrates a conventional image authentication method.

5. **Enhancing data security by secret sharing:-**Instead of hiding data directly into document image pixels, the explored method embeds data in the form of shares into the alpha channel of the PNG image. The effect of this may be regarded as double-fold security protection, one fold contributed by the shares as a form of disguise of the original image data and the authentication signals and the other fold contributed by the use of the alpha channel plane, which is created to be nearly transparent, as previously mentioned.

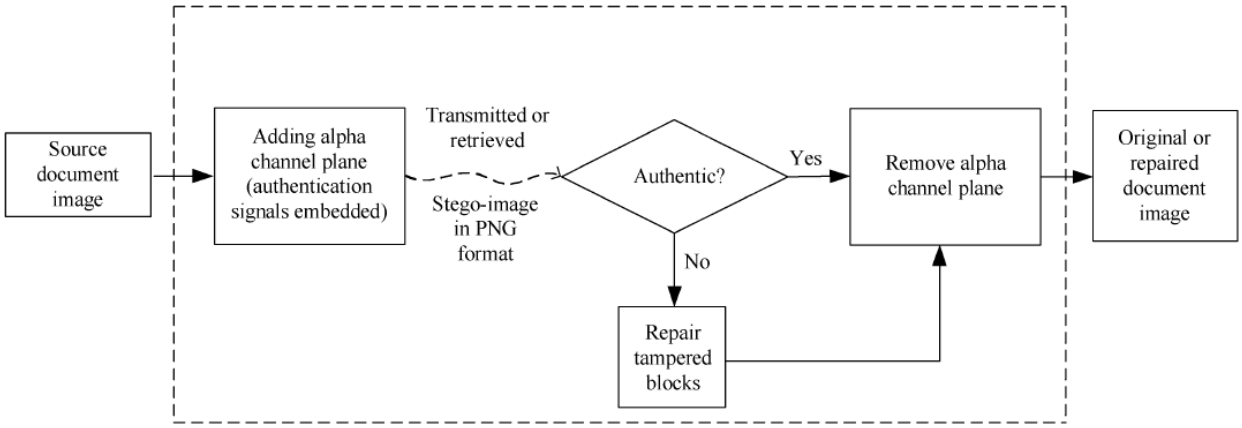


Figure 9.1: Framework of proposed document image authentication method.

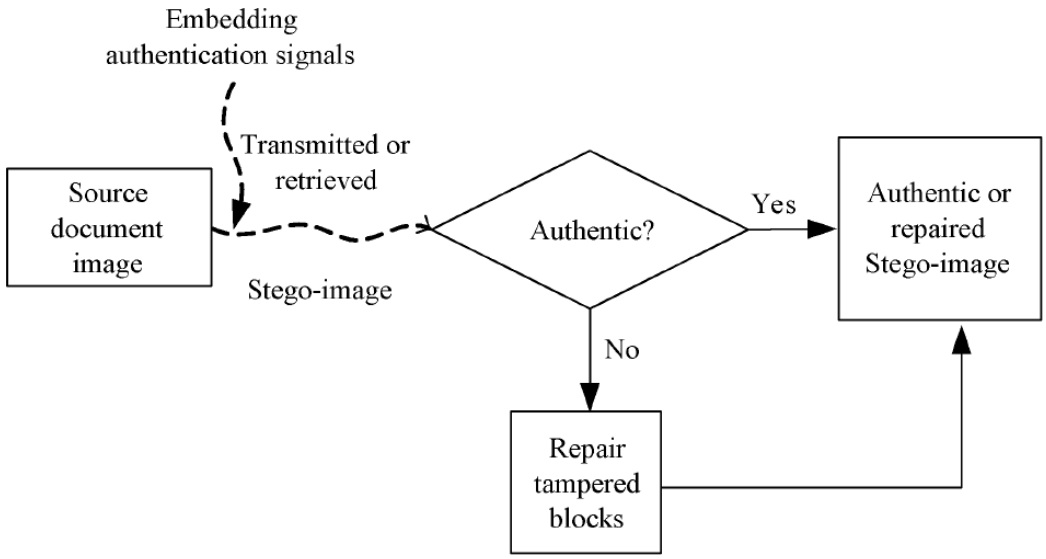


Figure 9.2: Framework of a conventional image authentication method.

9.2 Measures for Security Enhancement

The secret key K, which is used to randomize the pixel positions for embedding the mapped partial shares q_3' through q_6' mentioned in Step 9 of Algorithm 3, provides a measure to protect the shares. More specifically, as described in Algorithm 3, each block in the alpha channel plane may be regarded to consist of two parts, i.e., the *first part* including the first two pixels and the *second part* including the remaining four. The first part of each block is used for keeping the first two partial shares q_1' and q_2', and the second part for keeping the last four partial shares q_3' through q_6' of other blocks located at random positions. Therefore, the probability of correctly guessing the locations of all the embedded partial shares in a stego-image is $\frac{1}{[(m*n)-(m*n/6)/2]!}$, where mxn is the size of the cover image, $(m*n/6)$ is the total number of blocks, each with six pixels, and $[(m*n)-(m*n/6)/2]$ is the total number of pixels in the blocks other than those in the first parts of all the blocks. This probability is obviously very small for common image sizes, meaning that a correct guess of the embedded partial shares is nearly impossible.

To enhance further the security of the data embedded in the stego-image, one additional measure is adopted in the explored method. It is the randomization of the constant values

of x_1 through x_2 used in Step 6 of Algorithm 3 and Step 3(2) in Algorithm 4. Specifically, in Step 3(2) in Algorithm 4, we can see that the input shares into Algorithm 2, i.e.,$(1, q_1)$ and $(2, q_2)$, can be easily forged, leading to the possibility of creating fake authentication signals. To remedy this weakness, with the help of another secret key, we may choose these values of x_1 through x_2 for each block to be *random* within the allowed integer range of $0 \leq x_i \leq p(= 17)$ [11]. Then, the probability of correctly guessing all these values for all the $(m * n/6)$ blocks in a stego-image can be figured out to be $\frac{1}{(17*16*15*14*13*12)^{(m*n)/6}} \equiv \frac{1}{(8.911*10^6)^{(m*n)/6}}$,which is also very small for common image sizes $m * n$.

Chapter 10

Conclusion and Future Scope

10.1 Conclusion

The generated authentication signal and the content of a block have been transformed into partial shares by the Shamir method, which have been then distributed in a well-designed manner into an alpha channel plane to create a stego-image . The undesired opaque effect visible in the stego-image coming from embedding the partial shares has been eliminated by mapping the share values into a small range of alpha channel values near their maximum transparency value of 255. In the process of image block authentication, a block in the stego image has been regarded as having been tampered with if the computed authentication signal does not match that extracted from corresponding partial shares in the alpha channel plane. For the self-repairing of the content of a tampered block, the reverse Shamir scheme has been used to compute the original content of the block from any two untampered shares. Measures for enhancing the security of the data embedded in the alpha channel plane have been also used. Experimental results have been shown to prove the effectiveness of the used method.

10.2 Future Scope

1. Future studies may be directed to choices of other block sizes and related parameters (prime number, coefficients for secret sharing, number of authentication signal bits, etc.) to improve data repair effects.

2. Future studies may also explore the four levels of Moment-preserving thresholding method instead of two level Moment-preserving thresholding method for image binarization so as to form four level gray image from which the data for authentication and the repairing of grayscale images can be computed.

3. Future studies may explore the four levels of Moment-preserving thresholding method instead of two level Moment-preserving thresholding method for image binarization so as to form four level gray image from which the data for authentication and the repairing of true grayscale images can be computed.

4. Futher future studies may also explore the four levels of Moment-preserving thresholding method instead of two level Moment-preserving thresholding method for image binarization so as to form four level gray image from which the data for authentication and the repairing of color images can be computed.

References

[1] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579-1592, Oct. 2001.

[2] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.*, vol. 11, no. 6, pp. 585-595, Jun. 2002.

[3] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.*,vol. 14, no. 6, pp. 822-831, Jun. 2005.

[4] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans. Multimedia*,vol. 6, no. 4, pp. 528-538, Aug. 2004.

[5] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identiiĭnĄer," *IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741-744, Dec.2006.

[6] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving," *IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475-486, Apr. 2007.

[7] H. Y. Kim , " Secure authentication watermarking for halftone and binary images," *Int. J. Imag. Syst. Technol.*, vol. 14, no. 4, pp. 147-152, 2004.

[8] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement," *IEEE Commun. Lett.*,vol. 7, no. 9, pp. 443-445, Sep. 2003.

[9] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates," *IEICE Trans. Commun.*,vol. E90-B, no. 11, pp. 3259-3262, Nov. 2007.

[10] Y. Lee, H. Kim, and Y. Park, " A new data hiding scheme for binary image authentication with small image distortion," *Inf. Sci.*,vol. 179,no. 22, pp. 3866-3884, Nov. 2009.

[11] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[12] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *IEEE Signal Process. Lett.*vol. 73, no. 3, pp. 405-414, Nov./Dec. 2004.

[13] H. Yang and A. C. Kot, "Moment-preserving thresholding: A new approach," *Comput. Vis. Graph. Image Process.*, vol. 29, no. 3, pp. 377-393,Mar. 1985.

[14] Che-Wei Lee and Wen-Hsiang Tsai, "A Secret-Sharing-Based Method for Authentication Of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability," *IEEE transactions on image processing*, vol. 21, no. 1, January 2012.