International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Review on Methods of Authentication of Images with Data Repair Capability

Vrushali Chirmade[1], **Dimple Chaudhari**[2]

[1]Master Student, Electronics and Telecommunication, YTIET, Karjat, India

[2]Professor, Electronics and Telecommunication, YTIET, Karjat, India

Abstract: ***Image authentication methods based on conventional cryptography, fragile watermarking, semi-fragile watermarking and on image content signatures discussed in this paper. For each group of methods the type of the authentication tag, the dependency of this authentication tag on the image, the type of the authentication service provided are shown, that is: strict or content-based (selective) image authentication service, the localization capacity of the altered regions, as well as the possibility of restoration of image corrupted regions. Algorithms are also grouped according to the authentication tag that is used, and references are included. It can be noticed that one principal property of an image authentication system, the detection of malevolent manipulations. According to the summary table, algorithms performances are very similar. In fact, most of algorithms offer acceptable detection and localization of image manipulations while restoration performances still need to be improved.***

Keywords: cryptography, fragile watermarking, authentication tag, digital signature, hash function

1. Introduction

Digital images are used to preserve important information. But providing integrity and authentication to these images is a challenging task. In this era with the use of fast advanced technologies it is easy to modify the contents of these digital images. It is important to make an effective method to solve image authentication problem, particularly for document images such as important certificates, Scanned checks, art drawings, signed documents, circuit diagrams, design drafts, testaments etc. In the case of binary document images, it is difficult to authenticate because of its simple binary nature that lead to perceptible changes after authentication signal are embedded in the image pixel.

Image authentication techniques:
Before presenting and discussing various methods, we start by defining the general requirements that are essential for any authentication system. These requirements are:

- **Sensitivity:** The authentication system must be able to detect any content modification or manipulation. For strict authentication algorithms, detection of any manipulation is required and not only content modification.
- **Robustness:** Also called tolerance. The authentication system must tolerate content preserving manipulations. This property is valid just for algorithms that provide a selective authentication service.
- **Localization:** The authentication system must be able to locate the image regions that have been altered.
- **Recovery:** The authentication system must be able to partially or completely restore the image regions that were tampered.
- **Portability:** The authentication system must be able to carry the signature with the protected image during any transmission, storage or processing operation.
- **Complexity:** The authentication system must use real-time implemented algorithms that are neither complex nor slow.

2. Strict Image Authentication

Strict image authentication methods do not tolerate any changes in the image data. These methods can be further separated in two groups according to the techniques that are used: methods based on conventional cryptography and methods that use fragile watermarking.

2.1 Methods based on conventional cryptography

Image authentication methods based on cryptography compute a message authentication code (MAC) from images using a hash function. The resulting hash (h) is further encrypted with a secret private key S of the sender and then appended to the image. For a more secure exchange of data between subjects, the hash can be encrypted using public key K1 of the recipient. The verification process is depicted in Fig. 1b. The receiver computes the hash from the received image. The hash that was appended to the received image is extracted and decrypted using private key K1. The extracted hash and the calculated one are then compared. Techniques that are based on the hash computing of image lines and columns are known as line–column hash functions. Separate hashes are obtained for each line and each column of an image. These hashes are stored, and compared afterwards with those obtained for each line and each column of the image to be tested. If any change in the hashes is found, the image is declared manipulated otherwise it is declared authentic.Distortions localization can be achieved by identifying lines and columns for which the hashes are different. Unfortunately, the localization of changes can be

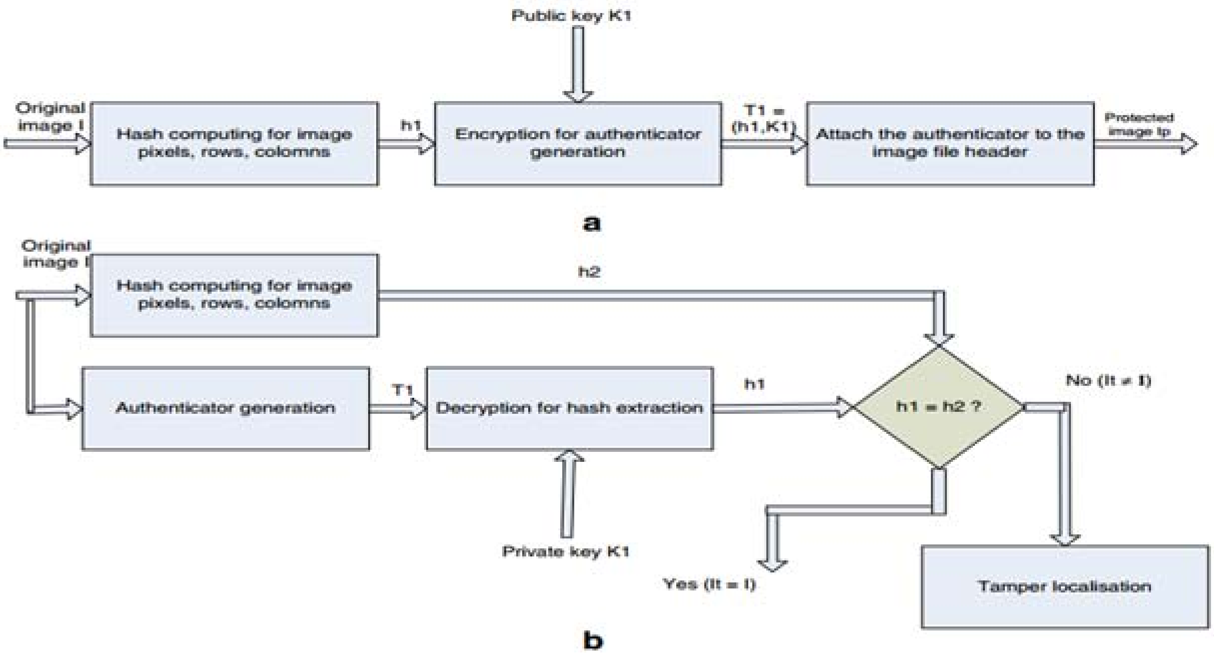
Public key K1
Original image I
Hash computing for image pixels, rows, colomns
h1
Encryption for authenticator generation
T1 = (h1,K1)
Attach the authenticator to the image file header
Protected image Ip
a
Original image I
Hash computing for image pixels, rows, colomns
h2
Authenticator generation
T1
Decryption for hash extraction
h1
h1 = h2 ?
No (It ≠ I)
Private key K1
Yes (It = I)
Tamper localisation
b

Figure 1: Strict authentication system by conventional cryptography; a. generation of authenticator; b. verification of authenticity

easily lost if more than one region of the image was corrupted.This is called the ambiguity problem of the line–column hash function.To solve this problem, another approach has been proposed by Wolfgang and Delp. This technique consists in obtaining the hash of image blocks, separately.If an image is to be tested, the user calculates the hashes for each block using the same block size, and compares the results with the hashes from the original image to decide whether the image is authentic. Blocks for which hashes are different enable tamper localization. The computation of hashes for each block separately had increased the localization capabilities. However, these techniques are not able to restore image regions that were tampered. Conventional cryptography was developed to solve the problem of message authentication, and had a great success since its appearance. Algorithms based on conventional cryptography show satisfying results for strict image authentication with high tamper detection. Localization performances are not very good but may be acceptable for some applications. Hash functions are very sensitive to any small change in the image pixels or even in the binary image data. In consequence the image is classified as manipulated, when just only one bit of this image is changed; this is very severe for most of applications.

2.2 Methods Based on Fragile Watermarking

2.2.1Fragile Watermarking using image information

Watermarking consists of calculating a watermark, hiding it in the image, and then extracting it when it is necessary. In this paper, we choose fragility as the basic criterion for algorithms classification. Fragile watermarking belongs to the strict authentication class, while semifragile watermarking to the selective authentication class. Some authors define reversible watermarking, also called erasable or invertible , as a subgroup of fragile watermarking. The idea behind reversible watermarks is to reconstruct the exact original image when the image is declared as authentic. Thus, it reconstructs the information that was lost during watermarking. Usually, it is alossless compressed version of the space where the watermark was embedded. This lossless compressed version is thereafter concatenated with the watermark, inserted within the image and extracted for reconstruction purposes only when the image is declared authentic. However, in most image watermarking algorithms, modifications caused by embedding functions are really insignificant. Therefore, reversible watermarks are desired only for specific applications such as for high sensitive images. Moreover, their main goal is to eliminate the distortion artifacts caused by the embedding functions. Throughout this paper we compare the restoration capabilities of each algorithm, which is somehow different from reversibility. Restoration is the ability of an algorithm to restore the damaged data. When an algorithm detects and localizes a region with some undesired manipulations, we wish that this algorithm could restore the original data. This requirement is desirable for wide range of applications.The basic idea behind fragile watermarking techniques is togenerate a watermark and to insert itin the image to be protected in such a way that anymodification made to the image is also reflected in the inserted watermark. Simply verifying the presence of the inserted watermark allows the image authenticity verification and eventually localization of tampered regions. This type of watermarking does not tolerate any image distortion. The image is considered authentic if and only if all its pixels remainunchanged.The first algorithms of fragile watermarking were based on watermarkgeneration from image information only as shown in Fig. 2a. The watermark is computed from a set of image pixels. The computation of the watermark differs between

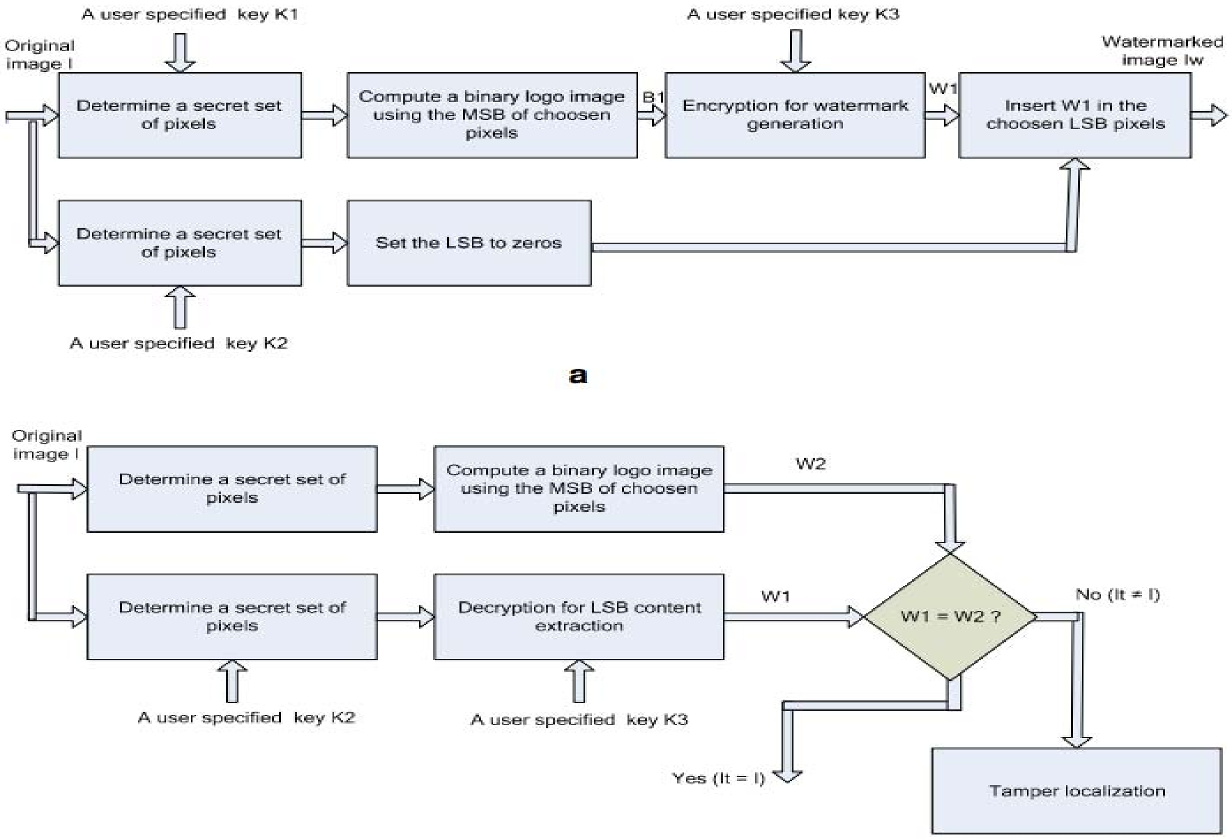
A user specified key K1
Original image I
Determine a secret set of pixels
Compute a binary logo image using the MSB of choosen pixels
B1
A user specified key K3
Encryption for watermark generation
W1
Watermarked image Iw
Insert W1 in the choosen LSB pixels
Determine a secret set of pixels
Set the LSB to zeros
A user specified key K2
a
Original image I
Determine a secret set of pixels
Compute a binary logo image using the MSB of choosen pixels
W2
Determine a secret set of pixels
Decryption for LSB content extraction
W1
W1 = W2 ?
No (It ≠ I)
A user specified key K2
A user specified key K3
Yes (It = I)
Tamper localization

Figure 2: Strict authentication system by fragile watermarking using image information; a generation of authenticator; b verification of authenticity

the various authentication methods. The set of pixels may be chosen with the help of a secret key K1. The computed watermark may be encrypted with a key K3.It is then inserted in the least significant bits of another set of pixels. In order to increase the algorithm security, the set of pixels where the watermark is embedded may be determined with another secret key K2. Similarly, the verification schema is shown in Fig. 2b. The secret keys must be known to the receiver, as well. The receiver uses the same key K2 to determine the set of pixels where the watermark is dissimulated in order to extract it. Also, the receiver uses the same algorithms to calculate the watermark from the received image and then compares the calculated watermark with the dissimulated one to decide whether the image is authentic or not. One of the first techniques that used image authentication by fragile watermarking was proposed by Walton; it used only image information to generate the watermark. This technique is based on the insertion, in the least significant bits (LSB), the checksum calculated with the grey level of the seven most significant bits of pseudo-randomly selected pixels. This method was able to detect and localize manipulations but with no restoration capabilities. Various algorithms were proposed for the realization of this technique.

2.2.2 Fragile Watermarking Using Watermark from Image and a Logo

In a more general schema, the watermark that is inserted inthe image to be authenticated is obtained by combining information from the image with a predefined logo as depicted in Fig 3a and 3b. A secret key K1 can be used to extract specific image information from the image. In order to generate the watermark, the extracted image information is combined with a binary logo by using another secret key K2. The computed watermark may be encrypted with a key K4. It is then inserted in the least significant bits of a set of pixels that may be determined with a secret key K3. The secret keys must be known to the receiver, as well. The receiver uses the appropriate key to determine the set of pixels where the watermark was dissimulated in order to extract it. Also, the receiver uses the same algorithms to calculate the watermark from the received image and then compares the computed watermark with the dissimulated one to decide whether the image is authentic or not.Strict image authentication is appropriate for many applications. For example, a modification of just one or twopixels in some medical or military images can dramatically change the decisions of doctors or war strategists, respectively,and can result in costly. Most existing image applications use image processing operations that preserve the content in order to save memoryspace and bandwidth or to enhance image quality: compression, geometric transformations and image enhancement techniques. So, some tolerant image authentication algorithms are needed.

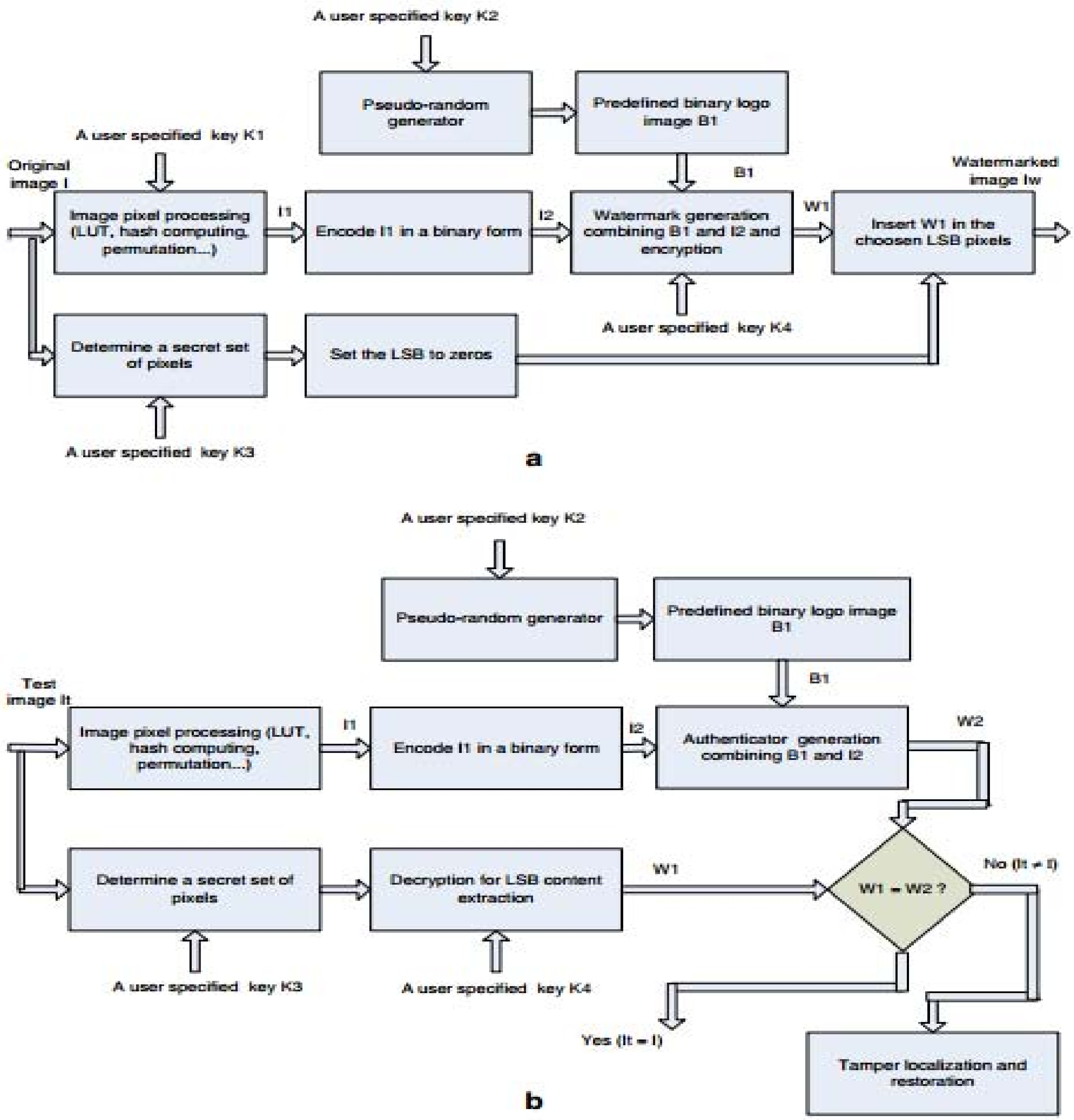
A user specified key K2
Pseudo-random generator
Predefined binary logo image B1
A user specified key K1
Original image I
B1
Watermarked image Iw
Image pixel processing (LUT, hash computing, permutation...)
I1
Encode I1 in a binary form
I2
Watermark generation combining B1 and I2 and encryption
W1
Insert W1 in the choosen LSB pixels
Determine a secret set of pixels
Set the LSB to zeros
A user specified key K4
A user specified key K3
a
A user specified key K2
Pseudo-random generator
Predefined binary logo image B1
B1
Test image It
Image pixel processing (LUT, hash computing, permutation...)
I1
Encode I1 in a binary form
I2
Authenticator generation combining B1 and I2
W2
Determine a secret set of pixels
Decryption for LSB content extraction
W1
W1 = W2 ?
No (It ≠ I)
A user specified key K3
A user specified key K4
Yes (It = I)
Tamper localization and restoration
b

Figure 3.Strict authentication system by fragile watermarking where the watermark is obtained from the image and a logo; a generation of authenticator; b verification of authenticity

3. Content-based Image Authentication or Selective Authentication

We defined a content modification as an object appearance or disappearance, a modification to an object position, or changes to texture, color or edges. We have also listed the image processing operations that preserve the image content. Thus, lot of applications that base their decisions on images need authentication methods that can tolerate content preserving manipulations while at the same time detect any manipulation that change the image content. This leads to newwatermarking methods known as semi-fragile watermarking, and to new approaches known as content-based signatures. In this section we will present and compare semi-fragile techniques and content-based signatures approaches that provide selective image authentication service.

3.1 Semi Fragile Watermarking

Robust watermarking is designed to resist all attempts to destroy the watermark. Its main application includes the intellectual property protection and owner identification. The robustness of the embedded watermark is crucial to resist any intentional and even unintentional manipulation. The goal of these techniques is not the verification of the image authenticity, but rather the verification of their origins. Conversely, fragile watermarking is designed to easily destroy the embedded watermark following any kind of manipulations of the protected image. It is useful for applications where strict authentication is needed, that is where the main objective is to determine whether the image has been modified or not, with the possibility of locating and reconstructing image regions that have been tampered. On the other hand, semi-fragile watermarking combines characteristics of fragile and robust watermarking techniques. Basically, the idea of semi-fragile watermarking is to insert a watermark in the original image in such a way that the protected image can undergo some specific image processing operations while it is still possible to detect malevolent alterations and to locate and restore image regions that have been altered. For image authentication purposes watermarking algorithms should be invisible. Visible watermarking algorithms are applied for on-line content distribution, transaction tracking or owner identification. The procedures of generating a watermark and embedding it into the image can be dependent on a private or public, symmetric or asymmetric, key system in order to increase the overall system security. This is a trade-off between security and computational time . Generally, symmetric key systems are less secure than asymmetric ones, and asymmetric key systems consume more resources and consequently need more computing time.The watermark is computed from the result of an image-processing algorithm applied on the image pixels. The computation of the watermark varies as different image processing algorithms can be used. A secret key K1 can be used to extract specific information from the image. In order to generate the watermark, the extracted image information is often combined with a binary logo using another secret key K2. Usually, the generated watermark is then inserted in a set of frequency coefficients that are in the middle range. The set of coefficients where the watermark is inserted may be determined with the help of a secret key K3. The computed watermark may be encrypted with a key K4. The secret keys must be known to the receiver, as well. The receiver uses the same key to determine the set of pixels where the watermark is dissimulated in order to extract it. Also, the receiver uses the same algorithms to compute the watermark from the received image and then compares the computed watermark with the dissimulated one to decide whether the image is authentic or not.

3.2 Image authentication by digital signatures based on the image content

Most recent investigations in the domain of image authentication were concentrated on digital signatures applied to the image content; these approaches offer high performance and promise additional breakthroughs in the near future. Such systems consist in (1) extracting specific high level characteristics from the original image; (2) applying a hash function to these characteristics in order to reduce their size; (3) digitally signing the hash value using an existing digital signature algorithm such as a private or public key system to increase the overall security; (4) attaching the signature to the original image or inserting it in the image using techniques for data dissimulation. Likewise, the verifying procedure of an image authenticity consists in (1) generating the image signature using the same algorithm; (2) extracting the attached or dissimulated signature; (3) comparing these two signatures using a comparison algorithm to decide whether the image was altered or not; (4) determining the image regions that were manipulated. When the image is declared as not authentic, information from the original signature could be used to partially or even completely restore the regions that were corrupted. Several parameters directly affect the performance of an image authentication system based on image content signature. These parameters include the choice of the appropriate characteristics, the choice of the hash function and the digital signature algorithm, the choice of the data dissimulation method in images as well as the choice of the algorithm that compares the signatures to decide about the authenticity of an image. Among these parameters, the image features that represent the image content and the data dissimulation method mostly affect the performance of image authentication methods. In fact, sensitivity, robustness, recovery, portability, safety and complexity are directly affected by the choice of the characteristics that are used to generate a content-based signature; they are affected as well by the choice of the data dissimulation method. The hash function and the digital signature algorithms are almost the same for all techniques. The algorithm used to compare the signatures directly depends on the selected characteristics and the dissimulation method. Therefore, we will use these two parameters, the choice of the appropriate characteristics and the data dissimulation algorithm, to classify and compare existing image authentication systems based on image content signatures.

4. Advantages and Limitations of Various Methods

Table 1 presents a summarized comparison of image authentication methods discussed in this paper: methods based on conventional cryptography, fragile watermarking, semi-fragile watermarking and on image content signatures. For each group of methods we have shown the type of the authentication tag, the dependency of this authentication tag on the image, the type of the authentication service provided, that is: strict or content-based (selective) image authentication service, the localization capacity of the altered regions, aswell as the possibility of restoration of image corrupted regions. Algorithms are also grouped according to the authentication tag that is used, and references are included. It can be noticed that one principal property of an image authentication system, the detection of malevolent manipulations. Moreover, the robustness against content preserving manipulations is not offered by the first two categories since they provide a strict authentication servicesand do not tolerate any modification to the original image.According to this summery table, algorithms performances are very similar. In fact, most of algorithms offer acceptable

Table 1: Comparison of the methods discussed in this paper

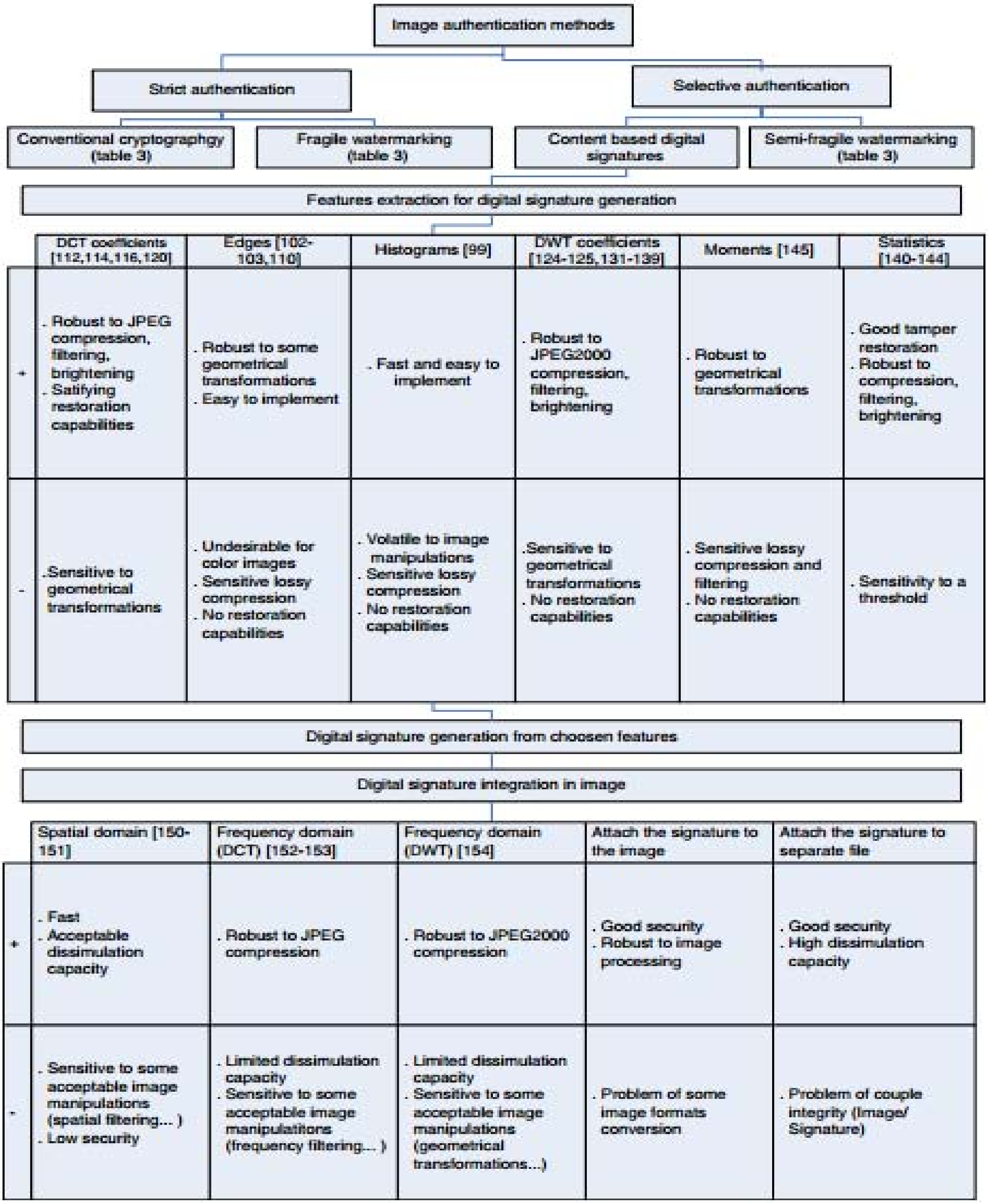

Image authentication methods

Strict authentication

Selective authentication

Conventional cryptographgy (table 3)

Fragile watermarking (table 3)

Content based digital signatures

Semi-fragile watermarking (table 3)

Features extraction for digital signature generation

	DCT coefficients [112,114,116,120]	Edges [102-103,110]	Histograms [99]	DWT coefficients [124-125,131-139]	Moments [145]	Statistics [140-144]
+	. Robust to JPEG compression, filtering, brightening . Satifying restoration capabilities	. Robust to some geometrical transformations . Easy to implement	. Fast and easy to implement	. Robust to JPEG2000 compression, filtering, brightening	. Robust to geometrical transformations	. Good tamper restoration . Robust to compression, filtering, brightening
-	.Sensitive to geometrical transformations	. Undesirable for color images . Sensitive lossy compression . No restoration capabilities	. Volatile to image manipulations . Sensitive lossy compression . No restoration capabilities	.Sensitive to geometrical transformations . No restoration capabilities	. Sensitive lossy compression and filtering . No restoration capabilities	. Sensitivity to a threshold

Digital signature generation from choosen features

Digital signature integration in image

	Spatial domain [150-151]	Frequency domain (DCT) [152-153]	Frequency domain (DWT) [154]	Attach the signature to the image	Attach the signature to separate file
+	. Fast . Acceptable dissimulation capacity	. Robust to JPEG compression	. Robust to JPEG2000 compression	. Good security . Robust to image processing	. Good security . High dissimulation capacity
-	. Sensitive to some acceptable image manipulations (spatial filtering...) . Low security	. Limited dissimulation capacity . Sensitive to some acceptable image manipulatitons (frequency filtering...)	. Limited dissimulation capacity . Sensitive to some acceptable image manipulations (geometrical transformations...)	. Problem of some image formats conversion	. Problem of couple integrity (Image/ Signature)

detection and localization of image manipulations while restoration performances still need to be improved. For strict authentication applications, where no modification to the original image is allowed, fragile watermarking algorithms perform better than algorithms based on conventional cryptography. Fragile watermarking algorithms offer high detection and localization capabilities. Moreover, some of them could provide an acceptable restoration level of damaged regions. On the other hand, selective authentication methods tolerate some desired manipulations while detecting any malevolent operations. Semi-fragile algorithms show good results for detecting and locating any malevolent manipulations while providing acceptable reconstruction performances. Unfortunately, their tolerance against desired manipulations includes mainly compression, noiseaddition and rotation by small angles, whereas, many of the desired manipulations need to be tolerated in practice. Since algorithms based on digital signature show more interesting results, we present them and compare their performances along with references in Fig. Figure presents a classification of image authentication methods with a detailed comparison of signature content-based methods. The comparison is made according to two important properties: the domain from which features are extracted to provide a content-based signature and the domain used to dissimulate or attach this signature. Moreover, for the sake of simplicity, only the most important weakness and strength for each group are highlighted. Every image-extracted feature used to generate the image signature has its weakness and force. The comparison of these features, their weaknesses and forces, help choosing the right method for a specific application. For example, if an application needs to tolerate compression with JPEG or JPEG2000 standard, the DCT domain or DWT domain, respectively, are best suited to generate the signature. If geometrical transformations need to be tolerated, the use of moments would be the best choice. If restoring the damaged data is important, statistical features could help well. Moreover, they are able to survive lossy image compression and a predefined set of content preserving manipulations (filtering, brightening...). On the other hand, using edges for content-based signature is undesirable for color images since one may change colors without affecting edges. This could result in an error where an image is declared authentic while some undesirable changes were introduced to it. Dissimulating signatures or attaching them to the image depends on the application and user requirements. A big dissimulation capacity and a high security can be achieved by attaching the signature to the image or to a separate file. However, the latter solution suffers from the problem of ensuring the couple image-signature integrity.

5. Problem Definition

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. 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.

6. Proposed Method

A method for the authentication of document images with an additional self-repair capability for fixing tampered image data is proposed. The input cover image is assumed to be a binary-like grayscale image with two major gray values like the one shown in Fig. After the proposed 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 proposed 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 proposed method is based on the so-called (k,n) -threshold secret sharing scheme proposed by Shamir in which a secret message is transformed into shares for keeping by participants, and when of 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.

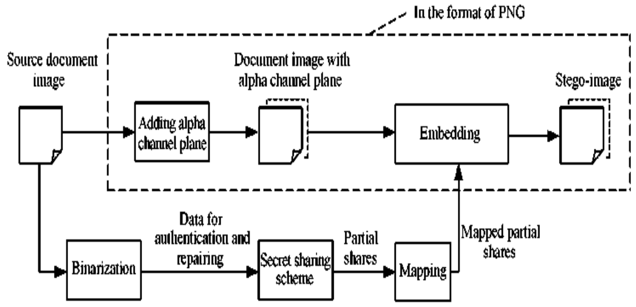

Figure 5: Creating a PNG image from a grayscale document image and an alpha channel

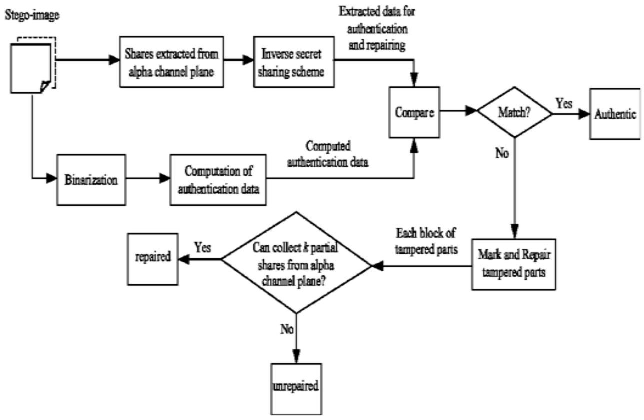
Stego-image
Shares extracted from alpha channel plane
Inverse secret sharing scheme
Extracted data for authentication and repairing
Compare
Match?
Yes
Authentic
No
Binarization
Computation of authentication data
Computed authentication data
Each block of tampered parts
Mark and Repair tampered parts
Can collect k partial shares from alpha channel plane?
Yes
repaired
No
unrepaired

Figure 6: Authentication process including verification and self-repairing of a stego-image in PNG format

Implementation platform:

Technical Requirement:

- Software Requirements:

Front End: Matlab2009b.

Operating system: WINDOWS-XP.

➢ Hardware Requirements:

Main processor :	Pentium IV processor 1.13 GHz.
Internal memory capacity:	128 MB
Hard disk capacity :	40GB.
Cache memory :	512 MB.

7. Conclusion

We have studied different conventional methods of image authentication. We have identified the problem. 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 proposed method problem of visual quality keeping is solved.

References

[1] C. Rey, and Dugelay(2002),"A survey of watermarking algorithms for image authentication", EURASIP journal on Applied Signal Processing, Vol. 6, pp. 24-32

[2] S. Radharani, M. L.Valarmathi(2010),"a study of watermarking scheme for image authentication", International Journal of Computer Imaging, Vol.12. No.4, pp. 24.32.

[3] R.G. VanSchyndel, A.Z. Tirkel and C.F. Os-borne,"A Digital Watermark" In Proceedings of IEEE International Conference in image Processing, vol.2, pp. 86-90,1994

[4] Ozgur Ekici., Bulent Sankur., "Comparative Evaluation of Semi Fragile Watermarking Algorithm", In Journal of Electronic Imaging, Vol 13,pp. 209-216, 2004.

[5] Digital Signature- Based Image Authentication" in 'Multimedia security: steganography and digital watermarking techniques for protection of intellectual property' (Idea Group Inc., 2003)

[6] C Yu, X Zhang "Watermark embedding in binary images for authentication", IEEE Trans. Signal Processing, vol.01, no.07, pp.865-868, September. 2004.

[7] 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 data repair capability" IEEE Trans. Image Processing., vol.21, no.1, january.2012.

[8] Niladri B. Puhan, Anthony T. S. Ho "Binary Document Image Watermarking for Secure Authentication Using Perceptual Modeling" IEEE International Symposium on Signal Processing and Information Technology2005.

[9] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, vol. 13.

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