



**HAL**  
open science

# A Novel Cholesky Decomposition-based Scheme for Strict Image Authentication

Wassila Belferdi, Lemnouar Noui, Ali Behloul

► **To cite this version:**

Wassila Belferdi, Lemnouar Noui, Ali Behloul. A Novel Cholesky Decomposition-based Scheme for Strict Image Authentication. 2nd international Conference on Pattern Analysis and Intelligent Systems, Nov 2016, Khenchla, Algeria. hal-03283303

**HAL Id: hal-03283303**

**<https://hal.science/hal-03283303>**

Submitted on 9 Jul 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A Novel Cholesky Decomposition-based Scheme for Strict Image Authentication

Wassila Belferdi  
Computer Science Department  
University of Batna 2  
05110 Fesdis Batna, Algeria  
Email: wassila.belferdi@univ-batna.dz

Lemnour Noui  
Mathematics Department  
University of Batna 2  
05110 Fesdis Batna, Algeria  
Email: nouilem@yahoo.fr

Ali Behloul  
Computer Science Department  
University of Batna 2  
05110 Fesdis Batna, Algeria  
Email: ali.behloul@univ-batna.dz

**Abstract**—With the increasing image falsification due to the easy access and use of image manipulation tools, image authentication techniques have seen considerable interest in protecting multimedia documents integrity and authenticity, it has been demonstrated to be a very powerful solution for ensuring the security of multimedia documents. The aim of this paper is to present a Cholesky decomposition based scheme for strict image authentication. To ensure the requirement of strict authentication where no changes are tolerated to the host image, the Cholesky decomposition properties are used beside the use of cryptographic hash function and public key cryptosystem. For the purpose of reducing the authentication data size, the diagonal of the Cholesky decomposition matrix is used instead of using the entire matrix.

The experimental results demonstrate that our technique is able to identify image tampering despite the minor modifications. In addition, the proposed scheme demonstrates its effectiveness in sensitive information systems. We review an application example in medical information security to ensure both integrity and authenticity. Our scheme can find a niche role in healthcare systems as an instrument for secure sharing and control of medical images.

**Index Terms**—Strict authentication, Cholesky decomposition, Cryptographic hash function, Public key cryptosystem.

## I. INTRODUCTION

In recent years, the security of multimedia documents becomes a serious problem, especially with the increasing image falsifications provided by the easy access and use of image manipulation tools. Thus, new information security requirements become ever more urgent [1].

Military, medical and quality control images must be protected against illegal use and unauthorized manipulations; which could affect the judgments based on these images. Thus, image authentication techniques has the ability to attain this requirement due to its effectiveness in several multimedia applications.

Generally, the image authentication schemes can be divided into tow main stages, stamping and verification stages. In the stamping stage the desired image to be protected is used to derive the authentication data that serves to verify the integrity of the image. At the verification stage, to decide whether the image is changed or not the consistence is evaluated between the authentication data calculated from the query image and the one calculated in the stamping stage [2].

Authentication schemes can be classified according to the service they provide into two main categories strict and selective authentication. In strict authentication schemes no modifications to the host image are accepted, even if only one bit is changed. It is used for several applications such as in law enforcement and medical image systems where no alterations in the image are allowed, while selective or content based authentication is used specifically when some image processing operations are allowed such as compression and filtering, it considers images as authentic when the content does not change [1]–[5].

Strict image authentication methods can be further separated into two main categories according to the techniques that are used: methods based on conventional cryptography and fragile watermarking-based methods [1], [3], [6]. The main difference between these two categories of techniques is that the former create a separate file to the authentication data, while the later embed it into the data to be authenticated [7].

In classical image authentication methods based on cryptography, an authentication data is computed from images using a hash function. The resulting hash is further encrypted with a secret private key of the sender and then appended to the image or stored in a confidential authority. During the verification process, the receiver computes the hash from the received image and compare it with the appended one [1], [6], [8]. To address both the authentication and integrity problems, a diversity of schemes has been proposed for different applications.

In this paper, a Cholesky decomposition-based scheme for strict image authentication is proposed, the novelty of our proposed scheme is the profit from the Cholesky decomposition properties to detect any modification made on the original image despite there imperceptibility by the human eyes.

Unfortunately the Cholesky decomposition is not possible and unique if the decomposed matrix is not positive definite, to solve this problem the given image is firstly multiplied by its transpose then decomposed by the Cholesky decomposition to generate an authentication data. Using the hash function the principal diagonal is hashed. This latter will be encrypted with the public key cryptosystem Rivest, Shamir, and Adleman (RSA).

To detect any modifications, the authentication data is

calculated from the given probe image and it is compared with the appended authentication data, depending on the consistence between the two sequences the image is considered as authentic or not.

Experimental results show the efficiency of our proposed method under several attacks and show the ability to use the proposed scheme in sensitive information applications such as low enforcement, military and medical images share and control.

The rest of this paper is organized as follows. In section II we describe the cryptographic background. Section III includes the related works and briefly formulates the problem in the existing methods. The Cholesky decomposition which will be used in the proposed scheme is described in section IV. The detailed proposed scheme is described in section V, then experimental results including an example of application are presented in section VI and VII respectively. Finally, section VIII concludes our work.

## II. CRYPTOGRAPHIC BACKGROUND AND TOOLS

Over the ages, Cryptography has attracted the attention as a tool to meet some of the information security requirements. Cryptography is the study of mathematical tools and techniques used in information security to provide a security service including confidentiality, data integrity, and entity authentication [9]. Enabling significant information to be stored or transmitted over non-secure networks, so that only authorized recipients can read it [1].

Message authentication techniques such as hash functions, private or public key systems and digital signatures are also used in image authentication and integrity systems [1]. There are several tools that are used in image authentication algorithms. The most important one is based on the hash function which afford an effective and secure information processing [1], [10].

### A. Hash Function

In modern cryptography, the cryptographic hash function is considered as one of the most frequently used primitives [9]. A hash function processes an arbitrary finite length input message to a fixed length output called the hash value or digest; in other words, it is the compact representation of the input message [1], [9], [10].

To achieve the security (cryptographic) requirement, a typically chosen hash function must satisfy at least, the following properties [10], [11]:

- For any given hash value  $y$  of  $H$ , it is “computationally impossible” to obtain a message  $m$  such that  $H(m) = y$ . It must be difficult to reverse  $H$  from  $y$  to get an  $m$  corresponding to  $y$ .
- For any given message  $m$ , it is “computationally impossible” to obtain any message  $m'$  such that  $m \neq m'$  and  $H(m) = H(m')$ .
- It is “computationally impossible” to obtain any two messages  $m$  and  $m'$  such that  $m \neq m'$  and  $H(m) = H(m')$ .

### B. Rivest, Shamir, and Adleman (RSA) Public Key Cryptosystem

One of the most used public key cryptosystem is the RSA cryptosystem. It is used to provide both secrecy and digital signatures, The security of this cryptosystem is ensured by the integer factorization intractability [9].

The RSA key generation, encryption and decryption algorithms are described as follows [9]:

1) *Key Generation Algorithm:* Each entity generates an RSA public key and a corresponding private key and do the following:

- 1) Generate two large distinct random primes  $p$  and  $q$  each roughly the same size.
- 2) Compute  $n = p \times q$  and  $\phi(n) = (p - 1) \times (q - 1)$ .
- 3) Randomly choose the integer  $e$  such that  $\text{gcd}(e, n) = 1$ .
- 4) Using the extended Euclidean algorithm (see [9]), Calculate the unique integer  $d$ ,  $1 < d < \phi(n)$ , such that  $e \times d \equiv 1 [\phi]$ .

The public key is  $(e, n)$  and the private key is  $d$ .

2) *Encryption Algorithm:* At the sender end,  $A$  encrypts a message  $m$  for the receiver  $B$ .

- 1) Obtain the authentic public key  $(e, n)$  of the receiver  $B$ .
- 2) Represent the message as an integer  $m$  in the interval  $[0, n - 1]$ .
- 3) Compute the encrypted message  $m_c \equiv m^e [n]$ .
- 4) Send  $m_c$  to  $B$ .

3) *Decryption Algorithm:*  $B$  should use the private key  $d$  to recover the plain text  $m$  from the encrypted message  $m_c$ .

- 1) Compute  $m \equiv (m_c)^d [n]$ .

## III. RELATED WORK AND PROBLEM FORMULATION

The emerging evolution of image processing tools imposes new challenges for researchers to design effective authentication schemes. The existing schemes should be further improved to meet new requirements including the use large-size authentication data and tolerating more image processing operations without compromising security.

The compromise between these requirements leads to a new generation of image authentication schemes that use new techniques to combine the watermark and digital signature techniques [7].

Friedman and Gary in [12] proposed the concept of trustworthy digital camera for image authentication. A hash function is used to hash the content of the original image, then the encrypted result is attached with the original image and sent to the receiver. To obtain the original digest, a public key is needed to decrypt the signature. The authentication of the images is verified by comparing the decrypted digest and the newly created one. In [13] a watermarking based image authentication scheme is proposed, that is suitable for several applications including medical images archiving and commercial image transaction. In this scheme, a private key is used to insert a watermark in the original image. To verify the image authenticity, anyone can use the public key to extract the watermark. If the watermarked image is modified

the visual quality of the extracted watermark will be affected. However, compared to the secret key schemes, the public key scheme are more expensive computationally [14]. Ping *et al.* described in [14] a secure visible watermarking-based scheme for ownership verification and authentication. According to the user need, the watermark can be visible or invisible. This scheme is able to detect any modifications made on the image. To check the ownership, a valid user key is required. The disadvantage of this scheme is that the secret key will need to be transmitted from the image owner to the user through a secure channel. In [15] a strict authentication watermarking-based scheme for medical images is proposed, the watermark is generated by hashing selected area of interest and embedded outside the region of interest in the LSB bits.

For strict image authentication, digital signature-based schemes are more applicable than watermarking-based schemes. The authentication data generated by the hash function is sufficiently short, enabling the fast creation of the digital signature. In addition, the hash function is very sensitive to any modifications made on the images, which means that changing a single bit in an image may result a different hash value. Moreover, the authentication data used to identify the image is associated with it in a separate file, by the sequence, the embedding capacity of those techniques is higher than the embedding capacity of watermarking-based schemes [7].

#### IV. CHOLESKY DECOMPOSITION

The Cholesky decomposition of a positive definite matrix  $A$  is a decomposition of the form:

$$A = L \times L^t$$

In which  $L$  is upper triangular with positive diagonal elements and  $L^t$  denotes the conjugate transpose of  $L$ , if  $A$  is positive definite; the decomposition is unique and there is only one lower triangular matrix  $L$  with strictly positive diagonal entries [16], [17].

##### A. Cholesky Decomposition Properties

The Cholesky decomposition is considered as an important tool in matrix computation because [17]:

- 1) It maintains correlated parameters; this means that the same information used to determine the value of one parameter is also used to partially conclude the value of the other.
- 2) The Cholesky decomposition destroy the relation between each parameter and their proceeding ones.
- 3) The Cholesky decomposition can indicate the correlation degree of its variables.
- 4) Compared with the other entries in a row, the size of the diagonal entries indicates the independence degree in a correlated variable.

This sort of result and properties can be potentially useful when considering the value of future research since this may give an indication of the degree to which variables are related.

#### V. PROPOSED METHOD

Our main issue in the proposed scheme is to address both the authentication and integrity of images. The use of Cholesky decomposition properties, is the major difference that differentiates our proposed scheme from existing state of the art approaches; correlated parameters of the Cholesky decomposition allows the control of any modification arise the factorized matrix; this means that modification that changes the value of one parameter will also partially affect the value of the other. In addition, the parameters correlation degree is indicated using the size of the diagonal entries, providing the use of the principal diagonal instead of using the whole matrix.

To fulfill the several requirements of security, the robustness of the proposed signature scheme is achieved by using the hash function and RSA cryptosystem that encrypts the obtained sequence before attaching it with the host image.

The goal of our proposed scheme is to detect any modification in the digital images. If the image is untempered, the recalculated authentication data and the attached one will be equal. If the image is tampered, the two extracted and attached authentication data will not be equal and the image considered as non-authentic.

Our proposed scheme consists of two processes: authentication data generation process and authentication verification process, which are described in the following subsections.

##### A. Authentication Data Generation Process

Let the original image  $I$  be an image with the size of  $M \times N$ . Detailed steps are described as follows, as depicted in Fig (1):

- 1) Cholesky decomposition is unique only if the matrix to be factorized is a positive definite matrix. Thus, to overcome this problem and obtain a positive definite matrix from the host image  $I$ , it is firstly multiplied by its transpose.

$$I_m = I \times I^t$$

- 2) Using the Cholesky decomposition, the obtained positive definite matrix  $I_m$  is decomposed into two Matrices  $L$  and  $L^t$ .

$$I_m = L \times L^t$$

- 3) Principal diagonal  $D$  of the  $L$  matrix is obtained.
- 4) The hash function is applied on the obtained principal diagonal  $D$ .

$$H = \text{hash}(D)$$

- 5) Using a private key, the hashed sequence is encrypted and attached with the original image.

So, an authentication data sequence (digital signature) can be transmitted electronically with the original image.

##### B. The Verification Process

As shown in Fig (2), to verify if the received image has tampered or not, the receiver computes the authentication data from the received image. The authentication data that was appended with the received image is extracted and decrypted using the public key  $K_p$ . The decrypted attached data and the calculated one are then compared.

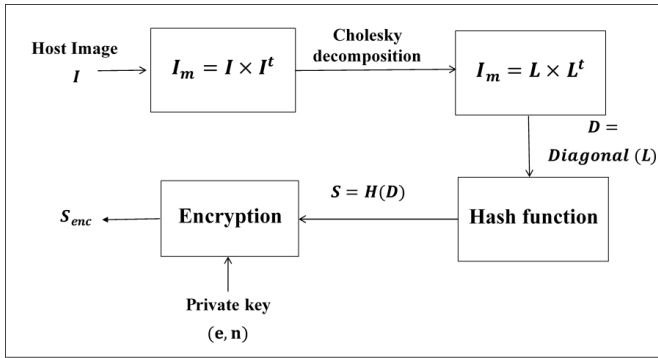


Fig. 1. Authentication data generation process.

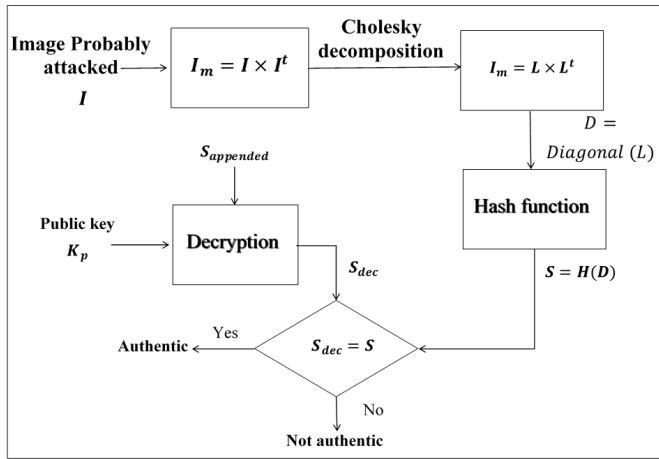


Fig. 2. Authentication data verification process.

If the two extracted and attached authentication data are equal the image is considered as authentic, else the received image is not authentic.

## VI. EXPERIMENTAL RESULTS

In our experiments, the testing programs are implemented using C++. Besides the use of Cryptoc++ library to call SHA256 hash function and RSA cryptosystem.

The performance of the proposed Cholesky decomposition based scheme is tested using a wide variety of images in the CVG-URG database such as “Baboon”, “Airplane”, “Girl”, “House”, “Lena” and “Peppers” with the size of  $256 \times 256$  pixels as shown in Fig (3).

In order to evaluate if the two authentication data sequences (the attached and recalculated) are equal or not, we use correlation metric as:

$$Corr(S_c, S_a) = \frac{\sum [(S_c(i) - \bar{S}_c) \times (S_a(i) - \bar{S}_a)]}{\sum \sqrt{[(S_c(i) - \bar{S}_c) \times (S_a(i) - \bar{S}_a)]^2}} \quad (1)$$

Where  $S_c$  and  $S_a$  are the calculated authentication data and the attached one respectively.  $\bar{S}_c$  and  $\bar{S}_a$  are the mean of the calculated authentication data and the attached one respectively.

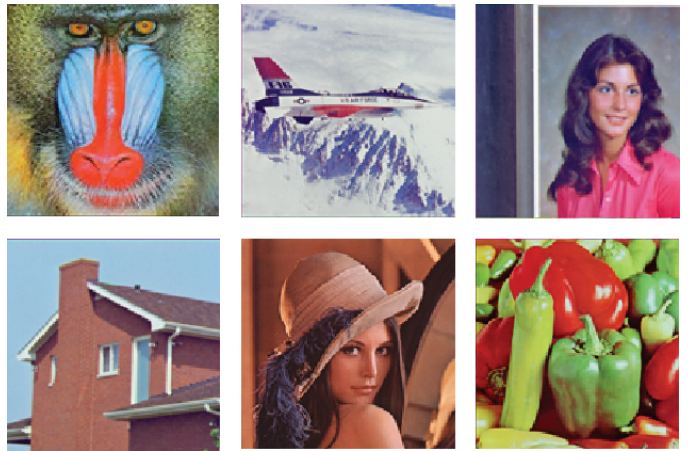


Fig. 3. Test images.

Generally, the correlation can take a value between 0 and 1. If it is closer to 1, the two sequences are getting more similar. In our tests, if the correlation is equal to 1 the image is considered as authentic, in the other case the image is considered as tampered.

The peak signal to noise ratio (PSNR) is defined in Eq.(2), in units of (dB), which may be used to evaluate perceptual distortion between the original and modified images.

$$PSNR = 10 \log \frac{N \times M \times \max(I(x, y))^2}{\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [I(x, y) - I'(x, y)]^2} \quad (2)$$

Where  $I$  is the original image,  $I'$  is the modified image, and  $N$ ,  $M$  denote the height and width of the image respectively. Generally, the larger the PSNR value is, the more invisible the distortions are.

To evaluate our algorithm, Table I, shows correlation values calculated between the authentication data attached to original images and the recalculated ones, to further demonstrate the advantages of our proposed method different attacks are performed.

As well seen from Table I, the proposed scheme proves its efficiency, without any modification made on the image the two sequences are similar and the correlation is equal to one.

In the other hand, changing only one bit from a pixel of the whole image changes the recalculated sequences and the correlation is different to one and closer to 0 despite the slight modification made.

For better illustration, results are also demonstrated under Salt and Pepper noise with a low variance equal to 0.0001, obtained results in Table I shows the effectiveness of the proposed method, where the correlation values remain low despite the PSNR high values greater than 46 (dB) which demonstrate that the slight modification made can't be perceptible by the human eyes but it can be detected using our proposed scheme.

## VII. APPLICATIONS

Our proposed method can find a main application in health-care systems, as an efficient tool for protecting sensitive

TABLE I

CALCULATED CORRELATION BETWEEN THE APPENDED SEQUENCE  $S_{appended}$  AND THE CALCULATED ONE  $S_{calculated}$  AND THE PSNR VALUES CALCULATED BETWEEN THE ORIGINAL AND THE MODIFIED IMAGES.

Attacks	-	Baboon	Plane	House	Lenna	Pepper
Without attack	Corr	1	1	1	1	1
Changing One bit	Corr	0.2996	-0.0181	-0.0921	0.0332	0.3067
	PSNR (dB)	96.2956	96.2956	96.2956	96.2956	96.2956
Changing One pixel	Corr	0.4038	-0.0955	0.2234	0.2353	-0.1673
	PSNR (dB)	62.8536	53.2498	51.8934	62.1441	55.1575
Salt and pepper variance 0.0001	Corr	-0.0361	0.1674	-0.1193	0.3033	0.1881
	PSNR (dB)	50.2796	48.7065	51.9702	48.6796	46.678

information such as military and medical images, the secure sharing and control of those images is needed. These images must be protected against any incidental or/and malicious manipulations, which could affect the judgments based on these images, especially in sensitive information applications.

To illustrate the efficiency of our proposed method in the medical images an example is shown in Table II.

From the obtained results of the correlation in Table II, we can conclude that any modification in the original images can be detected using our proposed scheme, even if the modifications can't be noticeable by the human (doctors) eyes.

### VIII. CONCLUSION

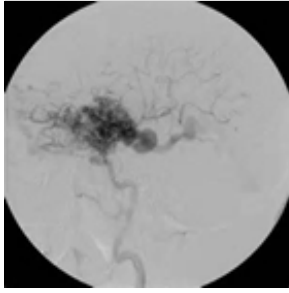
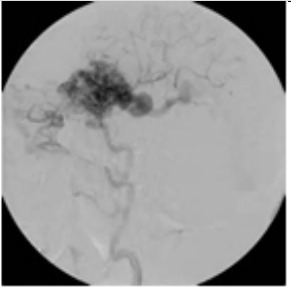
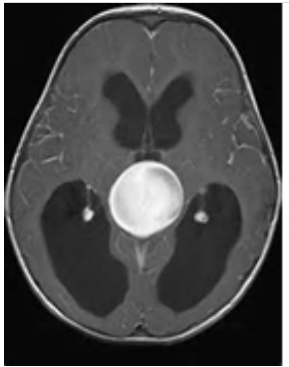
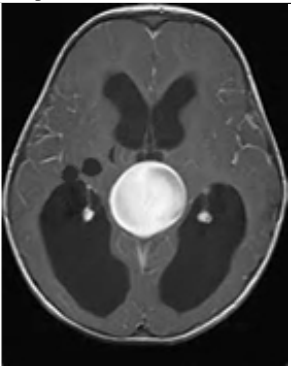
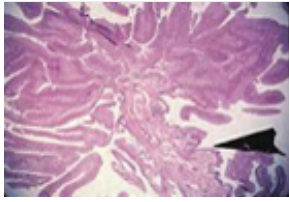
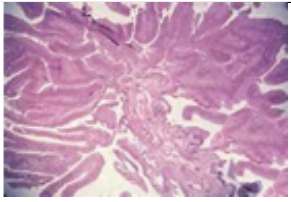
A novel Cholesky decomposition based scheme for strict image authentication has been proposed. By exploiting the Cholesky decomposition properties beside the use of cryptographic tools our proposed scheme shows an effectiveness in detecting tampered images. The proposed scheme can find its application in several areas, where sensitive information need to be protected such as various medical imaging modalities and services (radiology, surgery, etc.). Experimental results have shown the suitability of the proposed scheme for enhancing robustness and the security of protected images to provide an authentication service. Our future works turns around using the Cholesky decomposition properties to detect and restore tampered areas besides the exploitation of medical images properties to embed the authentication data into the host image.

### REFERENCES

- [1] A. Haouzia and R. Noumeir, "Methods for image authentication: a survey," *Multimedia tools and applications*, vol. 39, no. 1, pp. 1–46, 2008.
- [2] A. Tiwari and M. Sharma, "Comparative evaluation of semi fragile watermarking algorithms for image authentication," *Journal of Information Security*, vol. 3, no. 3, p. 189, 2012.
- [3] K. K. Doke and S. M. Patil, "Digital Signature Scheme for Image," *International Journal of Computer Applications*, vol. 49, no. 16, July, 2012.

TABLE II

AN EXAMPLE OF APPLICATION: CALCULATED CORRELATION BETWEEN THE APPENDED SEQUENCE  $S_{appended}$  AND THE CALCULATED ONE  $S_{calculated}$  AND THE PSNR VALUES CALCULATED BETWEEN THE ORIGINAL AND THE MODIFIED IMAGES.

Original images	Attacked images
	
PSNR=21.1895 (dB) $Corr(S_{appended}, S_{calculated})=-0.0968$ Decision:Tampered	
	
PSNR= 36.423 (dB) $Corr(S_{appended}, S_{calculated})=0.2590$ Decision:Tampered	
	
PSNR= 19.6475 (dB) $Corr(S_{appended}, S_{calculated})=0.06965$ Decision:Tampered	

- [4] N. Leelavathy, B. S. Priyatham, and S. S. Kumar, "A Watermark for Image Authentication using Mapping Code Book," *International Journal of Computer Applications*, vol. 93, no. 12, May, 2014.
- [5] C. REY and J.-L. DUGELAY, "Un panorama des mthodes de tatouage permettant d'assurer un service d'intgrit pour les images," *TS. Traitement du signal*, vol. 18, no. 4, pp. 283–295, 2001.
- [6] C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on Advances in Signal Processing*, vol. 2002, no. 6, pp. 1–9, 2002.
- [7] D.-C. Lou, J.-L. Liu, and C.-T. Li, "Digital signature-based image authentication," 2003.
- [8] C.-C. Lo and Y.-C. Hu, "A novel reversible image authentication scheme for digital images," *Signal processing*, vol. 98, pp. 174–185, 2014.
- [9] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.
- [10] P. Gauravaram and L. R. Knudsen, "Cryptographic hash functions," in *Handbook of Information and Communication Security*. Springer, 2010, pp. 59–79.
- [11] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics:

Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance,” in *Fast Software Encryption*. Springer, 2004, pp. 371–388.

- [12] G. L. Friedman, “The trustworthy digital camera: Restoring credibility to the photographic image,” *IEEE Transactions on consumer electronics*, vol. 39, no. 4, pp. 905–910, 1993.
- [13] P. W. Wong, “A public key watermark for image verification and authentication,” in *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, vol. 1. IEEE, 1998, pp. 455–459.
- [14] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE transactions on image processing*, vol. 10, no. 10, pp. 1593–1601, 2001.
- [15] J. M. Zain, “Strict authentication watermarking with jpeg compression (saw-jpeg) for medical images,” *arXiv preprint arXiv:1101.5188*, 2011.
- [16] N. J. Higham, “Analysis of the Cholesky decomposition of a semi-definite matrix,” 1990.
- [17] R. Edlin, C. McCabe, C. Hulme, P. Hall, and J. Wright, “Correlated Parameters and the Cholesky Decomposition,” in *Cost Effectiveness Modelling for Health Technology Assessment*. Springer International Publishing, 2015, pp. 119–132, doi: 10.1007/978-3-319-15744-3\_8.