8

2D Watermarking: Non Conventional Approaches

Hassen Seddik
ESSTT Higher Sciences and Technical School of Tunisia, Tunis Tunisia

1. Introduction

The growth of new image technologies and data exchanges, in addition to the ever-increasing use of multimedia content through online services, has created the need for new techniques capable of assuring copyright protection and data owner identification. Watermarking is now considered as an efficient means for resolving these problems. Watermark embedding techniques depend on the representation domain of the image (spatial, frequency, and multiresolution). Every domain has its specific advantages and limitations. Moreover, each technique in a chosen domain is found to be robust to specific sets of attack types. In addition all the techniques developed in theses domain are widely known and can be defeated to break the used algorithm and target the embedded watermark to destroy it or to put it out. So we need to develop another robust domain that defeats these limitations and respects all the watermarking criterions (capacity, invisibility and robustness). In this chapter, new watermarking methods are presented using new domains for the image representation and watermark embedding. These domains are based on different mathematical transformations of the image matrix. The applied transformations that process the image coefficients must dispose of three indispensable proprieties: no data loss, reversibility and preservation. Theses domains are found to be robust against a wide range of synchronous and asynchronous STIRMARK attacks. The robustness of the techniques in preserving and extracting the embedded watermark is proved after various attacks types. It is also improved when compared with other methods in use. In addition, the proposed methods are blind and the use of the host image is not needed in the watermark detection process.

2. A Blind image watermarking method based on the Hessenberg transformation

2.1 Introduction

The advent of the Internet brought about a sudden increase in the use of digital media in electronic commerce and various other services. Because of the ease of reproducing or falsifying digital media, it's very easy for the manufacturer to incur financial losses. To counter such problems, watermarking methods have gained significantly in popularity as they protect the ownership rights and simplify proprietor identification. To that end,

various techniques have been developed, each ultimately aiming at pinpointing equilibrium between imperceptibility and robustness of the watermark against wide attacks kinds, depending on the image domain representation. Many researchers have focused their efforts on security and robustness, as well as on the watermarking capacity that are essential to obtain an irremovable and inappreciable watermark with regards to the image processing domain. Each domain presents its robustness face to particular kind of attacks and its limitation to others, but no one is able to resist to a wide set of synchronous and asynchronous attacks gathering the robustness of the different domains. In addition, many of these techniques require the presence of the original image to read the inserted watermark. To satisfy these watermarking obligations, the necessity of either finding a blind watermarking method robust to a large set of attacks kinds, or a new image domain representation more robust than the known domains, is more and more urgent. In this chapter, these two constraints are satisfied. In fact we propose a new watermarking method using a new domain of the image representation based on the mathematical Hessenberg transformation. Using this method, both robustness and security criteria are fully met, and the embedded mark is fully invisible and present in all cases after different signal processing distortions. The Hessenberg Image Transformation brings a new representation domain with remarkable watermarking possibilities exceeding the limits of the domains cited above face to different attacks. The image is represented by the triangular part of the Hessenberg matrix used in the watermarking process. A study of this matrix is conducted with a view to identify the sectors or zones that can hold the watermark according to the three criteria mentioned above. Once the watermark is embedded in a chosen sector, inverse transformation is applied to return to the spatial representation holding the embedded mark.

If we explore the field of watermarking we find that the most commonly used watermarking technique domains are Spatial, DFT, DCT and Wavelet domains. There are many ways the spatial domain can be used in watermark embedding, for example: substituting the least significant bit in a chosen image pixel, coding by texture blocks, changing paired pixels, etc. However, various approaches that defeat the limitations of the spatial domains have been developed and can be used in the frequency domain. These include, the spread spectrum, content-based approaches, JPEG-based approaches, etc. For this purpose, the transformations used are the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT), and the Discrete Wavelet Transform (DWT). The DCT is the main transform used in JPEG image compression. It eliminates DFT high frequency components induced by the sharp discontinuities at the boundary between the consecutive periods in the time. To represent sharp value changes, it needs non-zero high frequency DFT components. For purpose of compression, all high frequency DFT components are deleted, causing a distortion of the original image. To overcome this difficulty, the DCT concatenates a period with the mirrored image of its an-adjacent period. The common DCT form is derived from a class of discrete Chebyshev polynomials. Whereas the advantage of DFT is its ability to describe the frequency responses of a signal even as allowing the possibility of extracting different signal characteristics from this frequency domain. While it's notable disadvantage is the absence of any information concerning the occurrence time of these frequency components. However, a particular frequency response that occurs in a certain interval can be detected with the Short Time Fourier Transform which splits the signal into fixed-length intervals where the Fourier analysis is applied. But if the cycle of the frequency response

exceeds the length of the fixed interval, it becomes impossible to describe it. To overcome this problem, the discrete wavelet transform is necessary by the use of base functions and windowing operations. In the case of data compression, the implementation of the DWT is similar to that of sub-band coding, where at each stage, a coarse overall shape and the details of the data obtained from the previous stage are derived. When encoding is performed in the DWT domain, two processes are applied: decomposition by separating data into frequency bands using high-pass and low-pass filtering, and down-sampling, which consists in removing unneeded data for future reconstruction. Decoding for its part, involves up sampling in order to adjust dimensionality and recombine data from different bands. Many methods are developed based on DWT schemes. One of the interesting is the use of the SA-DWT (Shape Adaptive Discrete Wavelets Transform) for developing a blind watermarking algorithm and HVS characteristics to achieve the best trade-off between invisibility and robustness. This method is found to be robust against some attacks such as lossy compression (JPEG, JPEG2000 and MPEG-4), scaling and filtering.

As explained, different domains are used for watermark embedding with various developed techniques. The spatial domain is found to be more robust against different kinds of asynchronous attacks such as rotation, rescaling, affine transforms etc. and less than others, whereas the frequency domains is well known for its robustness against synchronous attacks such as lossy compression (using DCT transform), filtering, noise adding or a specific kind of geometrical transforms such as scaling, rotation and translation (using Fourier-Melin transform or the multi-resolution domain: DWT). These limitations created the necessity to develop specific techniques in each domain to cover the robustness loss face to some attacks. In the following, we propose a new image watermarking domain: called the Hessenberg domain, which is able to counter a large set of different attacks kinds with high robustness, by the use of a substituting technique. We show that this domain can cover the limitations of the spatial, frequency and DWT domains. In addition, the robustness of this watermarking technique is improved when compared with many recent techniques in use.

2.2 Proposed Hessenberg watermarking technique

2.2.1 Mathematical Hessenberg transform overview

Any image can be transformed by an orthogonal transformation; we will illustrate the relationship between our proposed method and other transformations. In fact an orthogonal transform applies a rotation to the representation space. The data of the image passes from a space where they are highly correlated into a space where this correlation is minimized. The less correlated coefficients of the transformed image gather the image characteristics. If this information is classified in way of significance, the data can be compressed by eliminating the data which valuesare null or near to be null and by quantization of the selected coefficients to be transmitted. Let's note $T_{k,l}(i,j)$ a set of function of orthogonal discrete bases and $T^{*}_{k,l}(i,j)$ its complex conjugate. An image I of size M×N has a transformed form I_T given:

$$I_T(k,l) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I(i,j) T_{k,l}(i,j) \text{ Where } 0 \le k \le M-1 \text{ and } 0 \le l \le N-1 \quad (1)$$

$$I(i,j) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I_T(k,l) T^*_{k,l}(i,j) \text{ Where } 0 \le i \le M-1 \text{ and } 0 \le j \le N-1 \quad (2)$$

From these transformations an important characteristic must be illustrated which is the energy distribution. In Figure 1, we show an example of the energy distribution in the spatial and frequency DCT domains. We will illustrate the importance of the energy distribution of the image through the Hessenberg transform and its affect in the watermarking process.

The proposed method uses the mathematical Hessenberg transformation. The used algorithm is based on the LAPACK routines for computing the Hessenberg form of the processed matrix. Perhaps the most successful numerical algorithm for computing the complete eigensystem of a general square matrix A is the implicitly shifted QR algorithm. One of the keys to the success of this method is its relationship to the Schur decomposition:

$$A = U T U^* \quad (3)$$

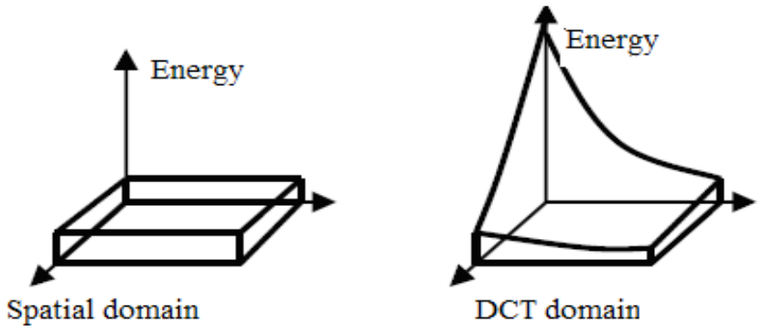


Fig. 1. Energy distribution in the spatial and transformed domains.

This well-known decomposition asserts that every square matrix A is unitarily similar to an upper triangular matrix T. The QR algorithm produces a sequence of unitary similarity transformations that iteratively reduce A to upper triangular form. In other words, it computes the Schur decomposition. A practical implementation of the QR algorithm begins with an initial unitary similarity transformation of A to the condensed form $Q^* A Q = H$ where H is upper Hessenberg (almost upper triangular') and Q is unitary. Then the following iterations to set the lower triangular to zero is performed as follows:

$$Q^* A Q = H \text{ is first factorized} \quad (4)$$

For j=1, 2, 3… until convergence. Select a shift μ then the QR factorization is as follows:

$$VR = H - \mu I \quad (5)$$

Then the matrices Q and H are assigned the following values:

$$\begin{cases} H = V^* H V \\ Q = QV \end{cases} \quad (6)$$

In this scheme, V is unitary and R is upper triangular (i.e., the QR factorization of $H - \mu I$). It is easy to see that H is unitarily similar to A throughout the course of this iteration. The iteration is continued until the sub-diagonal elements of H converge to zero, i.e., until the Schur decomposition has been (approximately) obtained. To summarize these mathematical steps, we can say that in finding the eigenvalues of a matrix using the QR algorithm, the matrix is first transformed by a unitary similarity transformation to upper Hessenberg form. The QR algorithm then iteratively generates a sequence of upper Hessenberg matrices by unitary similarity transformations. For general real matrices, Q^* becomes Q^T and the routine reduces the real general matrix A to the upper Hessenberg form H by this orthogonal similarity transformation:

$$A = Q\,H\,Q^T \text{, where Q is a unitary matrix so that } \quad Q^T Q = I\ (size(A)) \tag{7}$$

I: denotes the identity matrix and Q^T represents the unitary matrix transpose. The general matrix structure produced by the routine is presented by the following equations as $H(i,j) = 0$ unless $i = j$ or $i = j - 1$ and:

$$H = \begin{bmatrix} a_{11} & a_{12} & . & . & a_{1n} \\ 0 & a_{22} & & & a_{2n} \\ . & & . & & . \\ . & . & & . & . \\ 0 & . & & 0 & a_{nn} \end{bmatrix} \tag{8}$$

The form of H will be tri-diagonal if the processed matrix is symmetric or Hermetian. In general, the mathematical application of this transformation serves two purposes: the first is to obtain a matrix having the same eigenvalues as the original one, but which requires less computation to reveal them; conversely, the second is the packed storage. In fact, a triangular matrix may be stored more compactly, if the relevant triangle is packed by columns in a one-dimensional array.

The a_{ij} elements of H are stored in the one-dimensional array W as:

$$a_{ij} = W\left(i + j\left(j - 1\right)/2\right) \quad for \quad i \le j \tag{9}$$

In this work, the produced triangular Hessenberg matrix is exploited as a new representation domain of the image where the watermark is embedded. By analyzing this matrix, we discovered the existence of an exploitable zone. Embedding a watermark in this zone produces no effect on the original matrix values after applying the inverse Hessenberg transform. This zone provides imperceptibility and robustness to the watermark. To take advantage of this characteristic, we apply this transformation to the image matrix to obtain the Hessenberg triangular representation of the image. This matrix is processed to find in which zones we can embed a watermark without any change produced on the original image. This means that we can change and increase the values of this zone in the Hessenberg matrix, without any effect being produced on the original image after the inverse Hessenberg transform is applied. The following section presents the study applied to this matrix to identify this zone called insensitive zone.

2.2.2 Hessenberg matrix study

Successive iterations as shown in the following figure decreases the original matrix values from upper region to the lower one.

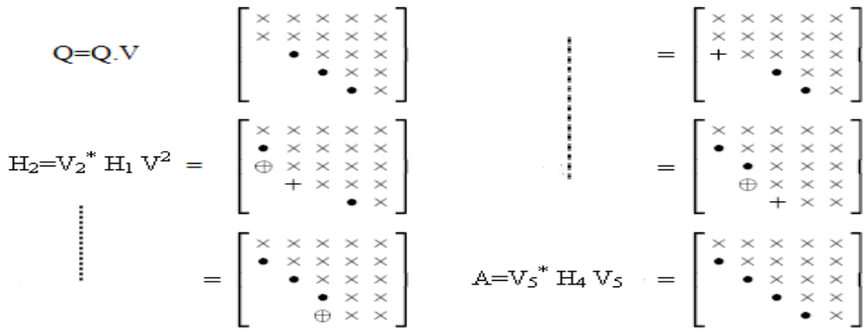


Fig. 2. Successive iterations of the H matrix.

These iterations tends to set the values of the lower triangular part of the Hessenberg matrix that we will call H matrix to zero. As a consequence, the values of the upper part of the Hessenberg matrix follow the sense of this decrease. The values of the matrix H decrease from the upper left sub-diagonal to the lower right sub-diagonal as shown in Figure 3, 4 and 5, containing a pick in the upper left part which values are in the range of 2 to 3.10^4 as shown in figure 6. The first figures 3, 4 and 5 are illustrated without this pick.

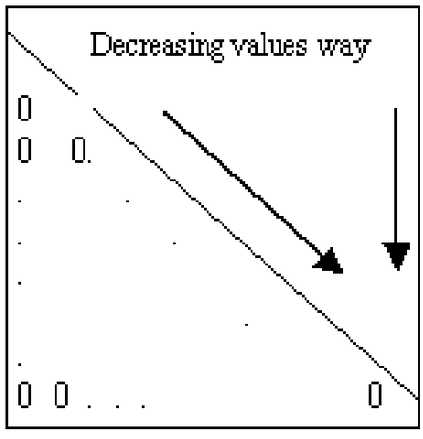


Fig. 3. Direction of decreasing matrix values.

The unidirectional value decrease is an important characteristic of this transformation. In fact, it is helpful in the matrix zones study. It allows the upper triangular part of the matrix to be divided into different blocks, in the way of the decreasing values. In analogy with the image matrix, the energy of the image is concentrated in the mid-high and high part of the transformed Hessenberg matrix. The mid-low and lower part of this transformed matrix contains a low energy of the image while its values are the weaker in the matrix. While the Hessenberg transformation is an orthogonal transformation similarly to DCT, we will

exploit the previous detailed characteristics to determine different Hessenberg matrix bands that can characterize the Hessenberg transform with respect to their effect on the image quality if a watermark is embedded. In this study the processed blocks are rectangles of 5 pixels high and 20 pixels wide. They are respectively examined with an overlap of 10 pixels from left to right and 2 pixels from top to bottom. In order to determine the bands or zones that produces the same effect on the image if they are processed, the study consists of substituting each selected block B by a supposed small watermark W and then applies the inverse Hessenberg transform in order to come back to the spatial representation and view the effects of each block change on the image distortion. After sliding over the entire matrix and testing all the blocks, we set the limits of the insensitive zone. This zone represents the matrix sectors for which values change or increase does not affect the original image. It is exploited for watermarking purpose. This study revealed the existence of other three zones detailed in the next section.

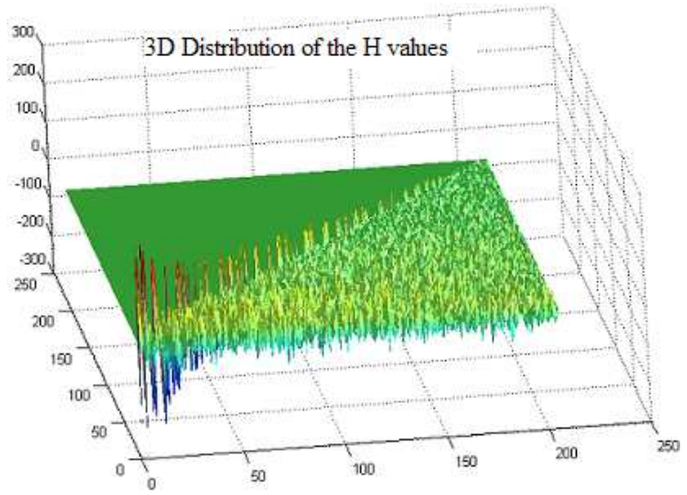


Fig. 4. A 3D distribution of the H matrix values

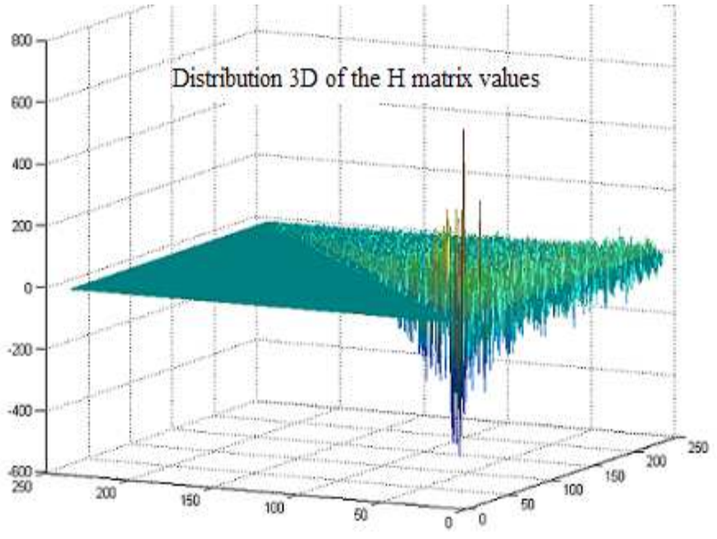


Fig. 5. Representation of the decreasing H values.

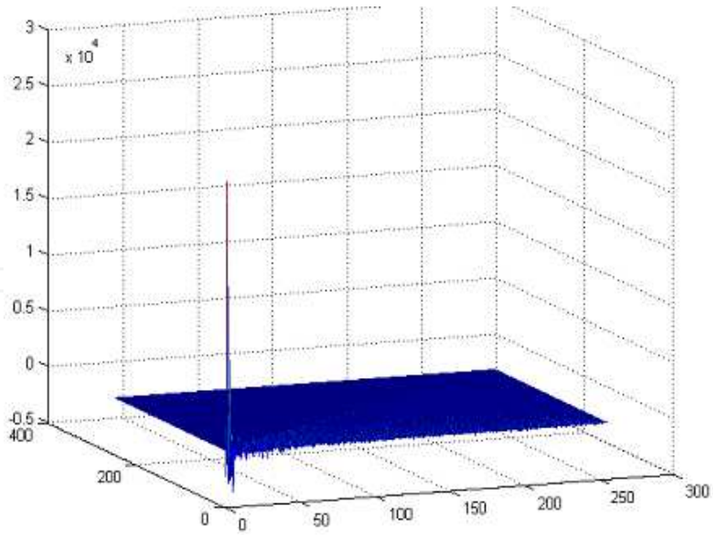


Fig. 6. Representation of the pick in the H matrix.

2.2.3 The watermarking process

The watermarking process consists in substituting one or multiple blocks in the Hessenberg matrix with a watermark. Once these blocks are substituted, the inverse transform is applied to the watermarked matrix in order to return back to the original image hiding the inserted watermark. To simplify the watermarking process, the watermark consists in applying a non-random permutation function on the chosen block values. The same function turns the obtained values to the nearest integer. The embedded watermark is then multiplied by a gain factor. This factor is chosen with respect to the limits of the image quality preserve. The substitution procedure is shown in Figure 6 and in equations (10)-(14).

Let B be the designed block, H the Hessenberg matrix, n the number of blocks that partitions the matrix and B'_k the watermark block:

$$H = \{ B_i \} \ as \ i \in [1, n] \tag{10}$$

H is composed by a set of n associated blocks:

$$\mathrm{H} = \{\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3, ..., \mathrm{B}_k, ..., \mathrm{B}_n\} \tag{11}$$

$$W = A(B_k) \tag{12}$$

A is a function used to apply a non-random mixture on the block values and turning them to the nearest integer value, W is the obtained watermark having the same size as B_k.

$$B'_k = K \ w \tag{13}$$

K is a gain factor used to increase the watermark values in order to add more resistance against attacks. The transformed Hessenberg matrix H' that holds the substituted watermark becomes:

$$H' = \{B_1, B_2, B_3, ..., B'_k, ..., B_n\} \quad (14)$$

To preserve the image quality and to guarantee that the embedded watermark is kept imperceptible, it is important to choose "very well" the matrix zone where blocks are substituted. Indeed from this zones study, a partition of the Hessenberg matrix in four zones is carried out with respect to the image quality change due to the block substitution, as shown in Figures 7 and 8.

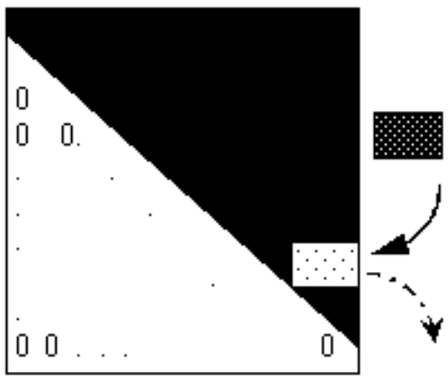


Fig. 7. a) The matrix blocks substitution.

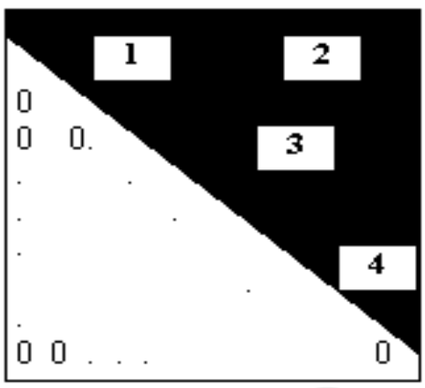


Fig. 7. b) The matrix partition.

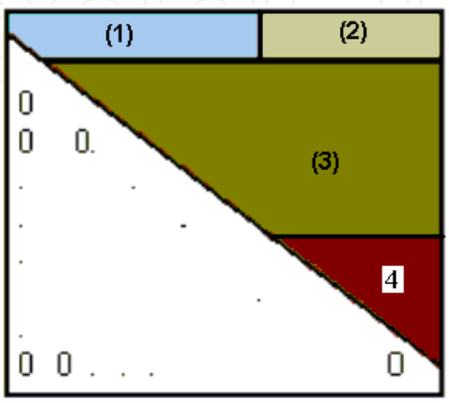


Fig. 8. Matrix delimited zones.

The Hessenberg transform is an entirely reversible transform that brings the image from the spatial representation to the H matrix and come back without any information loss or change. If this transform is applied on the image several times the same matrices are generated. This data preservation allows us to apply it on the image and use its transformed matrix for watermarking purposes. The Hessenberg matrix is divided in four zones. Each zone produces a specific distortion effect on the image if it is modified. The first zone containing the highest values in the transformed matrix and then contains the main part of the image energy. This zone is represented by the first twenty lines from the top and 150 columns from the left. Substituting blocks in this region of the Hessenberg matrix, affects considerably the image quality by adding to it a distortion look as presented in section 4. The second zone is situated between the first twenty lines from the top and a width between columns 150 and 256; this is a sensitive zone for image watermarking because any change in its values damages the original image considerably by adding to it a blurred effect. The intensity of the blur depends on the gain factor strength used. The first and second zones at the top and the fourth zone at the bottom delimit the third zone shown in Figure 8. In this zone, any watermark embedding followed by an inverse Hessenberg transform, damages the image by adding a noise effect to it. In fact the forms and shapes in the obtained image do no change, but a noise speck appears locally or in the entire image depending on the position of the substituted blocks. The intensity of this noise depends essentially on the magnitude of the gain factor used. Of course in these three mentioned zones if a low gain factor is used as it preserves the range of the watermark values near to the original matrix coefficients no change appears in the image. The fourth zone, which is red, is delimited between lines 160 to 256 in width and between columns 155 to 256 in height, excluding the lower triangle zero values. This zone contains the lower values of the matrix as presented in figure 1c; week energy of the image is transformed and spread in this zone. Because of the decreasing values direction in the Hessenberg matrix, this zone has the smallest values in the entire matrix. It is found to have an insignificant effect on the image quality whatever the change in its values and the increase in the gain factor. In this zone, different sectors can be substituted by a watermark. In our simulations, the sector delimited between lines 220 to 253 and columns 230 to 256 is used. As a result, the watermark insertion will consist in embedding a watermark block in this fourth Hessenberg zone as shown in figure 9 and 10. The gains factor increases up to 35 without any distortions to the watermarked image. Then, embedding a watermark in this zone allows us to increase the watermark robustness against different attacks. The visual imperceptibility threshold is not exceeded and the image quality is preserved. To supply more security, a secret key is provided to the copyright owner, used to determine the position of the watermarked sector.

Based on the detailed previous study, the choice of the embedding zone and the selected block to be substituted with the watermark block is chosen. It must increase the robustness of the embedded watermark against a large set of attacks and decreases the distortions introduced to the watermarked image. The fourth zone in the Hessenberg matrix is found as it satisfies these essential constraints to develop the watermarking algorithm. After watermarking the Hessenberg matrix, an inverse process shown by the following equation is applied to come back to the spatial representation of the image as follows:

$$\ddot{I}_W = inv(Q)\ \mathrm{H}'\ \mathrm{inv}\left(\mathrm{Q}^{\mathrm{T}}\right) \tag{15}$$

Where $\ddot{I}_W$ is the watermarked image, H′ the watermarked Hessenberg matrix and Q is the unitary matrix. The watermark-embedding algorithm is presented in Figure 5.

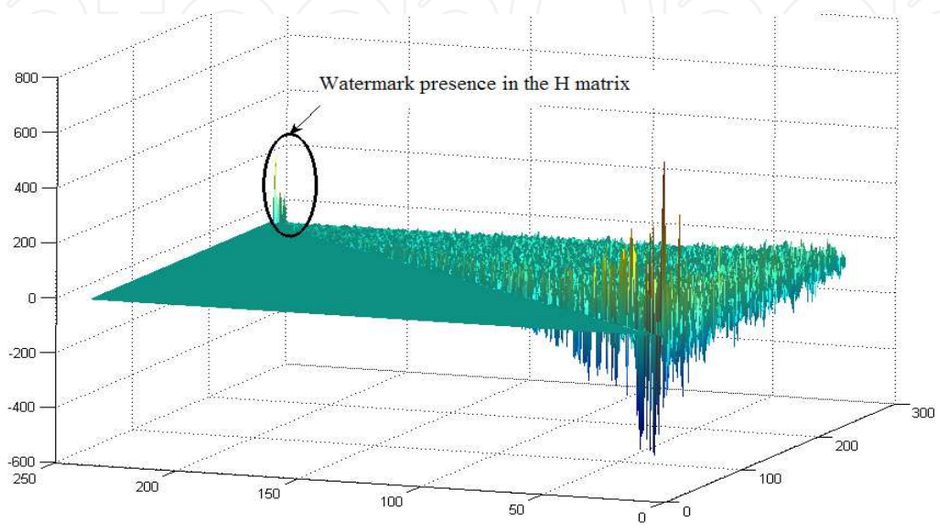


Fig. 9. The embedded watermark in the Hessenberg matrix.

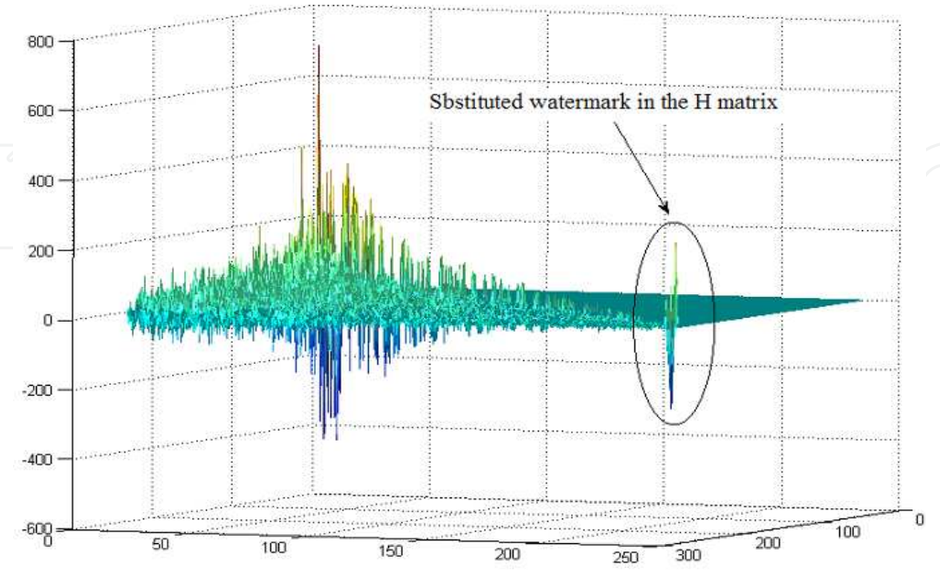


Fig. 10. Block watermark substituted in the fourth zone of the H matrix.

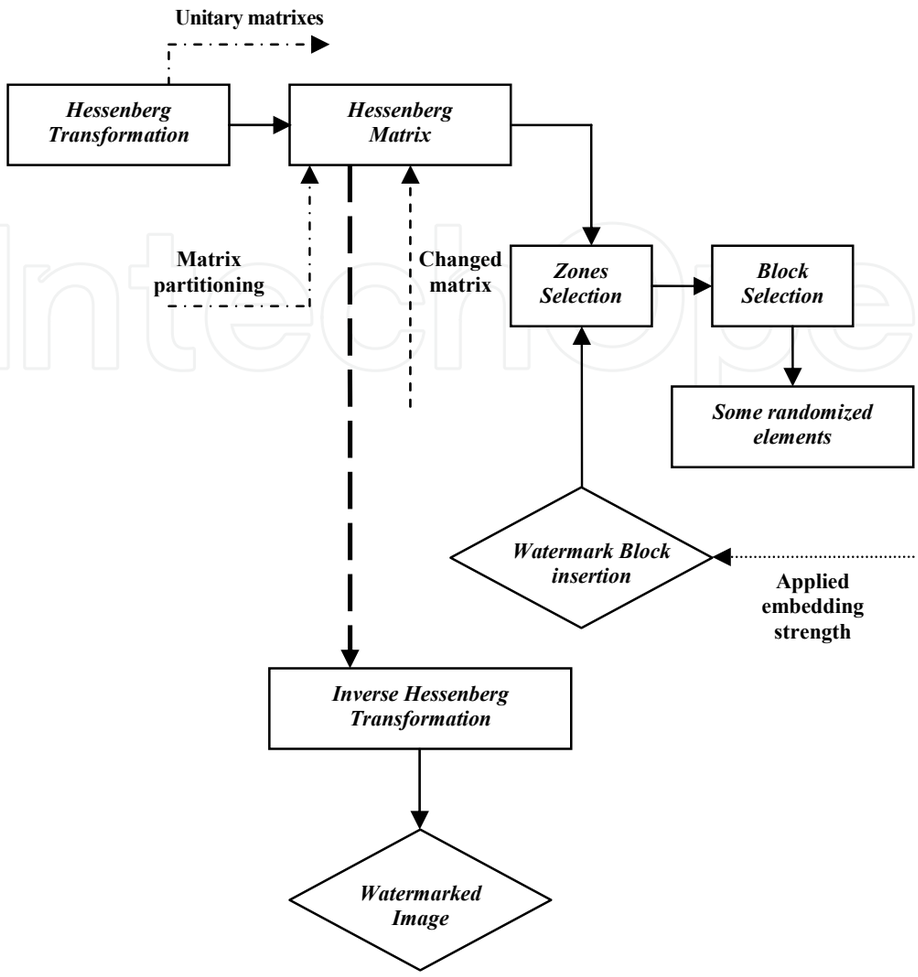


Fig. 11. The Hessenberg watermark embedding algorithm.

2.3 Watermark recovery and tests

In order to test the watermark presence, the Hessenberg transformation is applied on the watermarked image to handle the transformed Hessenberg matrix. The secret key is used to detect the position of the watermarked sector. Once this sector is located, the similarity between the extracted and the original watermark (W′ and W) is determined. The watermark extraction procedure is detailed in figure 6. Two measures of performance can be computed, the first is the (BER) bit error rate as false positive or false negative detection errors. The false positive detection is a false alarm of an incorrect detected watermark. While the false negative detection error consists in a missed detection of an existent watermark. The probabilities of these two types of errors are derived based on a first-order autoregressive image model as shown by:

$$P_{fp} = \frac{1}{2}\, erfc\left(\frac{T\sqrt{N}}{\sigma_w\ \sigma_{\mathrm{I}}\ \sqrt{2}}\right) \text{And}\ \ P_{fp} = \frac{1}{2}\, erfc\left(\frac{\left(\sigma_w^2 - T\right)\sqrt{N}}{\sigma_{\mathrm{I}}\ \sqrt{2}}\right) \tag{16}$$

Where $erfc\,(x) = \frac{1}{\sqrt{2\Pi}} \int_{x}^{\infty} e^{-t^2/2}\, dt$, σ_w and σ_I are the watermark and image variances, N is the total number of pixels in the watermarked image and T is the detection threshold over which the watermark is set as detected. While the location of the watermark in the Hessenberg matrix is known by the use of the secret key, the second measure based on the normalized correlation is more appropriate in this work. This measure is presented in (17), where n and m are the watermark block size.

$$Corr = \frac{\sum_{1}^{n}\sum_{1}^{m} W\, W'}{\sqrt{\left(\sum_{1}^{n}\left(\sum_{1}^{m} W^2\right)\ \sum_{1}^{n}\left(\sum_{1}^{m} W'^2\right)\right)}} \tag{17}$$

To test the robustness and the improvement that our method offers, different STIRMARK attacks are applied on the watermarked image. Once the image is attacked, a correlation is computed between the original watermark block and the attacked one. A threshold T_h fixed equal to 0.85 is applied to decide whether the watermark is detected or not. This threshold is chosen as the mean of the total correlation values corresponding to all synchronous and asynchronous attacks applied on the watermarked image in the simulation study. Some of these tests that provide week results corresponding to some geometrical attacks are not displayed in Table 1. The used attacks and gathered correlation results are detailed in Table 1. The chosen sector and applied gain factor, giving the best correlation result without causing any visible distortions between the original image and the watermarked one, are shown in the same table. The results prove the high resistance of this method against different attacks, especially JPEG compression, noise adding and convolutions filtering Stirmark attacks. In addition, an improvement against other attacks is noted when compared with other current techniques as shown in figures 18 and 19. Various examples of those attacks are simulated below on the original cameraman image followed by the corresponding peak detection of the watermark block between 1000 other random blocks. The watermark embedding capacity depends on the required embedding procedure. For a robust watermark embedding only the fourth Hessenberg zone is used. We can embed in the other zones for a fragile watermark embedding method using a low gain factor that avoids damaging the image quality. To establish a more quantitative measure of imperceptibility, we make use of the peak signal to noise ration (PSNR) metric. This measure serves generally as a good rule for the watermark visibility estimation, given by:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\left(I_i - \ddot{I}_{Wi}\right)^2 \tag{18}$$

$$PSNR = 10\log_{10}\frac{255\times 255}{MSE} \tag{19}$$

Where MSE is the mean square error, N is the total number of pixels in the image, I and $\ddot{I}_W$ are the original and watermarked image. With K is used equal to 35 and embedding in the fort zone. The PSNR of the watermarked image is maintained in the range of 40–50 dB (so

that $\ddot{I}_W$ is visually indistinguishable from I). Generally if the distortions between two images output a PSNR higher than 35 dB, no differences are visually detected. In this work, the computed PSNR from the experimental study is equal to 44.55 dB using the cameraman image, 49.70 dB using the image door and 44.62 dB using the image blood.

	STIRMARK ATTACKS	Correlation values		STIRMARK ATTACKS	Correlation values
1	Convolution filter 1	0.9138	**2**	Adding Noise 0	1
3	Convolution filter 2	0.9994	**4**	Adding Noise 20	0.9662
5	Compression JPEG 20	0.9603	**6**	Adding Noise 40	0.8811
7	Compression JPEG 40	0.9704	**8**	Adding Noise 80	0.7671
9	Compression JPEG 60	0.9802	**10**	PSNR 10	1
11	Compression JPEG 70	0.9891	**12**	PSNR 50	1
13	Compression JPEG 80	0.9925	**14**	Remove lines 60	0.8412
15	Compression JPEG 90	0.9999	**16**	Rotation 2°	0.7789
17	Compression JPEG 100	1	**18**	Rotation 45°	0.8641
19	MEDIANCUT 5	0.7538	**20**	Rotation 90°	0.9124
21	MEDIANCUT 7	0.8634	**22**	Affine 7	0.9876
23	MEDIANCUT 9	0.7565	**24**	Affine 5	0.9941

Table 1. Watermark detection responses values (Substituted Block dimension and location: [220:253,230:256], Gain factor: K = 35).

JPEG quality factor	20	40	60	70	80	90	100
PSNR (dB)	23.943	24.581	24.979	25.168	25.373	25.607	25.760

Table 2. PSNR variation against different JPEG quality factor attacks.

Median Filter size	5×5	7×7	9×9
PSNR (dB)	21.528	20.831	20.381

Table 3. PSNR variation against Median filtering attack.

Noise level	20	40	60	80
PSNR (dB)	25.763	8.374	6.826	6.015

Table 4. PSNR variation against different noise level adding attack.

The PSNR is also computed between the original image and the different watermarked attacked images. The PSNR variation against different attacks level as JPEG compression, median filtering and noise adding are present in tables 2, 3 and 4. The watermark extracting using the inverse procedure is shown by figure 12.

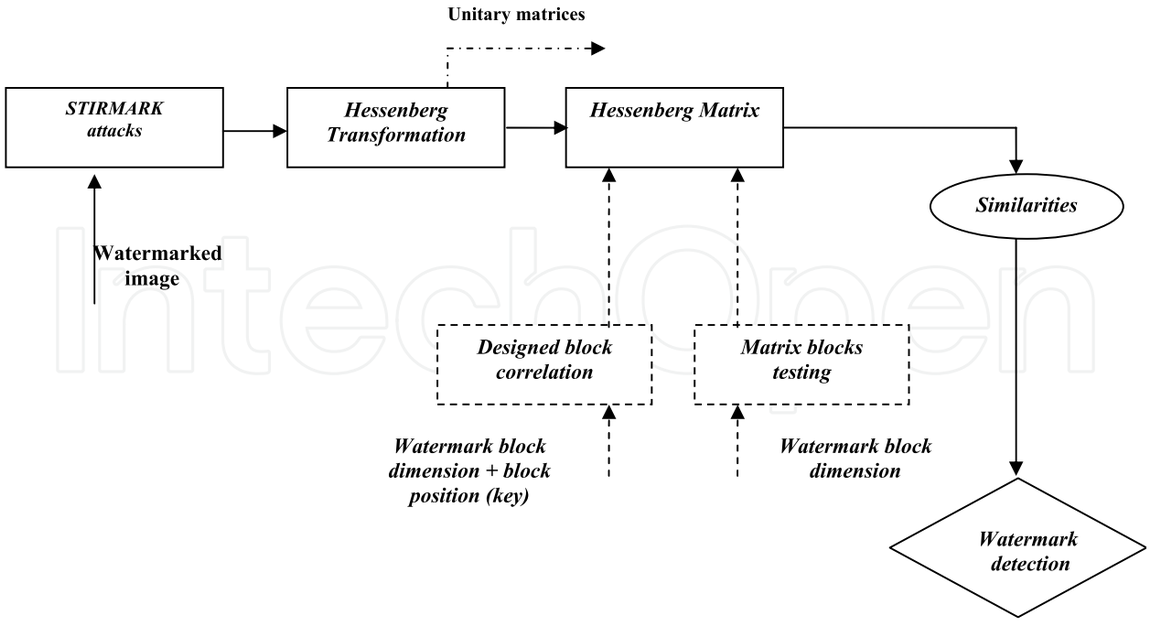


Fig. 12. The watermark blind detection algorithm after the applied attacks.

2.4 Experimental results and discussion

The results prove the high resistance of this method against different kinds of attacks such as: JPEG compression, noise, rotation, affine transform and other Stirmark attacks. Using this method we exploit the advantages of being robust face to different kind of attacks in the same time we have the guaranty of a secure and undetectable watermark with a rapid embedding and extraction algorithm. After applying the Hessenberg transform on different attacked images we note the values of the H matrix are nearly invariant if the fixed gain factor in the embedding procedure is not exceeded. This explains the fact that the watermark is always detected. The maximum error values resulting from the difference between the H matrix of a watermarked image and this of a watermarked and attacked image by JPEG compression indexed 40 are contained in the range between 7 and 9 in the entire matrix excluding the upper left matrix corner. The matrix resulting of this difference is shown in figures 13. This error pick value varies in the range of 2.10^3. With regard to this error value occurring in the upper part of the first zone, the error resulting in the zones 2 and 3 represents a ratio limited between 4 and 5.10^{-3}. The fourth zone presents an error band between the watermarked image and the attacked one contained in the range between -2 and 3 as shown in figure 14. This means that the numerical difference resulting between the watermarked image and the watermarked attacked one in this zone is too week. This difference presents the error resulting from the applied attack. This resulting error presents a ratio of 1.10^{-3} when compared with the error pick in the first zone. This week variation in the embedding zone with regards to the other zones composing the H matrix preserves the watermark from loss. On the other hand, the mathematical characteristics concerning the successive iterations of the Hessenberg transform bringing the values of the lower triangular part to zero and transforms the image matrix into a triangular matrix which absolute values varies from 2.10^4 to 0. We can say that the energy of the image is concentrated in the upper and middle zones. That is why embedding in the fourth zone introduces a week energy to

the image and then a high embedding strength is needed to introduce distortions to the watermarked image.

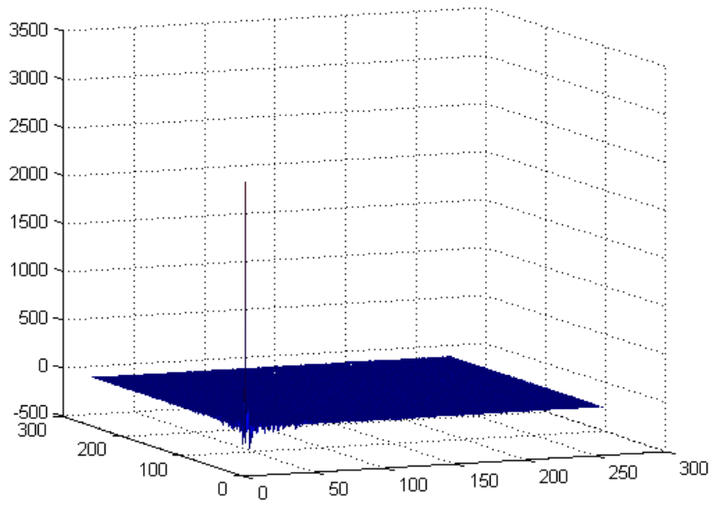


Fig. 13. Difference resultant between two *H* matrices belonging respectively to a Watermarked image and JPEG 40 lossy compression attacked image.

Figure 15 and 16 illustrate the presence of the watermark in the fourth zones after the watermarked image has been attacked by JPEG 40 compression and convolution 2 filtering. Because of the very week variation of the Hessenberg values in the watermarking zones if compared with the others matrix zones, the watermark is always preserved from loss after attacks.

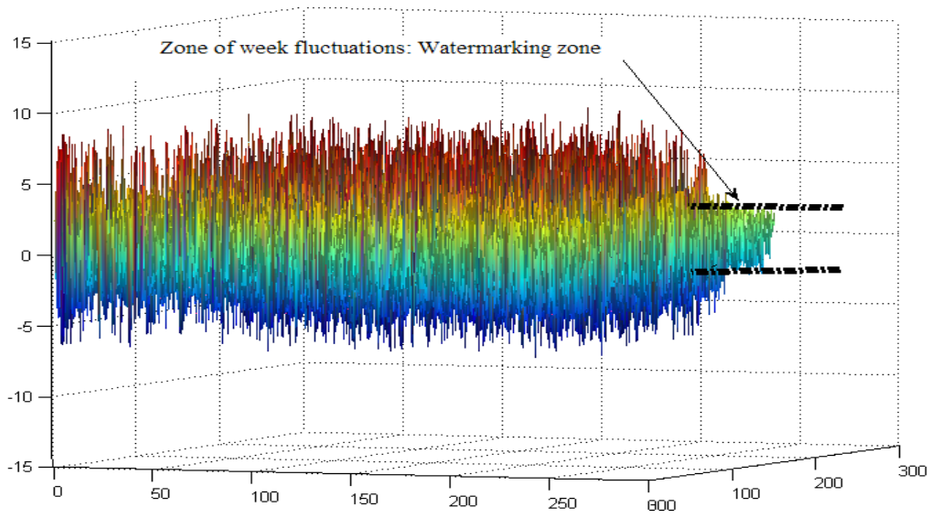


Fig. 14. Error band between the H matrices corresponding to zones 2, 3 and 4.

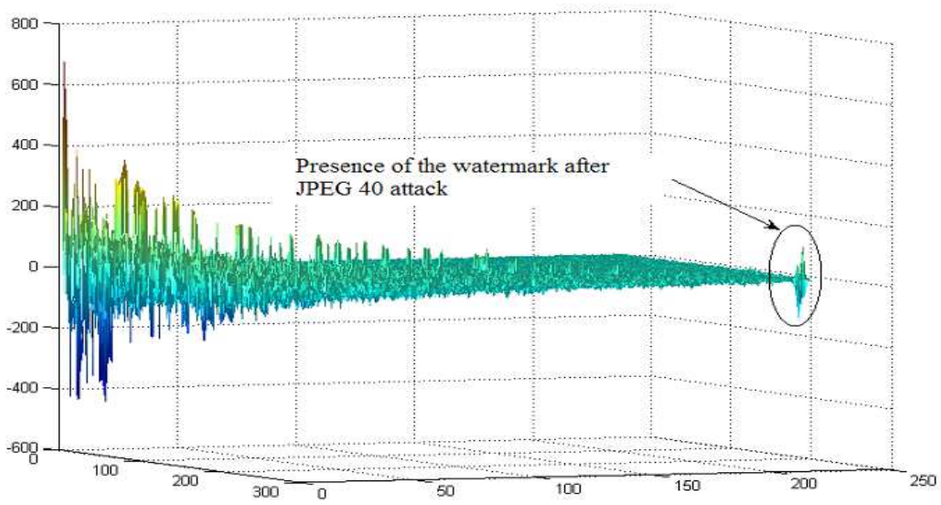


Fig. 15. Watermark presence in the H matrix after JPEG 40 attack

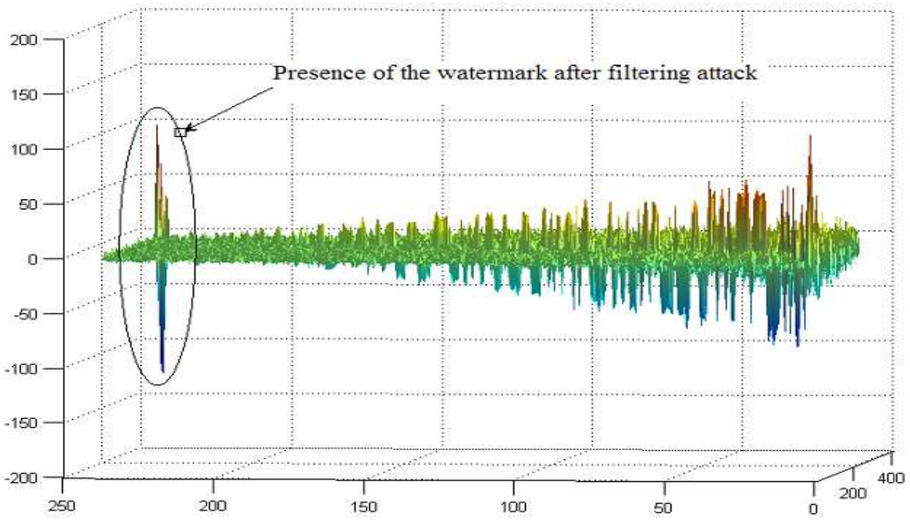


Fig. 16. Watermark presence after Convolution filtering 2 attack.

As shown in figure 18, the proposed method is also more robust to JPEG compression than recent algorithms. From JPEG 70 to JPEG 50 the CHEN algorithm is slightly higher then our algorithm, Nevertheless, when using high compression rates such as JPEG 20 and JPEG 10 the proposed method maintain its robustness by preserving the embedded watermark. The other methods lose their resistance face to this destructive attack. In the same time, when compared with other methods using the DWT domain, high robustness against noise adding is presented. The additional robustness to convolution filtering and different geometrical distortions is also presented. The proposed Hessenberg method provides also a better robustness face to median filtering then many other techniques as shown in figure 19.

Figure 17, presents the correlations values computed between the extracted watermark after seven JPEG compression attacks and the original one, with different quality factors from JPEG 100 to JPEG 20.

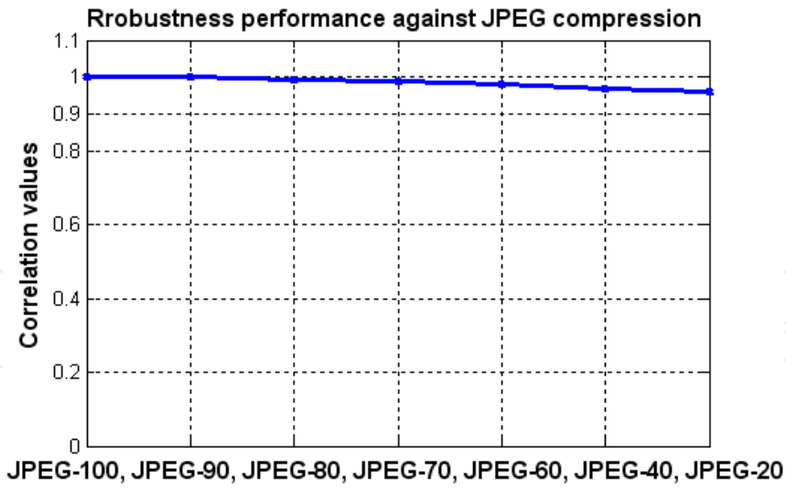


Fig. 17. Robustness of the Hessenberg technique against JPEG compression quality.

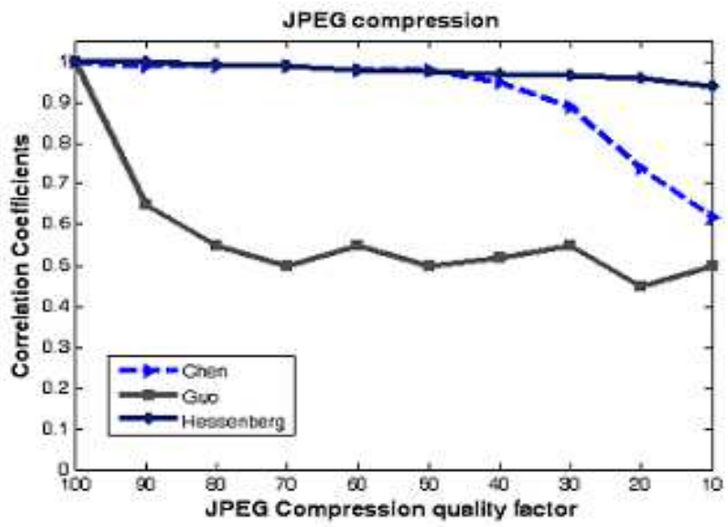


Fig. 18. Robustness variation face to JPEG compression.

As we shown in table 1 this technique is visibly more robust against synchronous attacks than geometrical ones. In fact the synchronous attacks applied on the image modify the values of its intensity values. After applying the Hessenberg transform on it we will extract the same H matrix with a variation of its values from a zone to another. Of course as we demonstrated in the previous section, the fourth zone has the less variation in the entire matrix and that is why we find high robustness if we embed in this zone. Conversely, if an asynchronous attack is applied on the watermarked image a change in the pixels position will happen. Since the Hessenberg transformation is a block-based orthogonal transform, the change in the image pixels position will be reflected on the Hessenberg matrix. The position of the values of the H matrix corresponding to the location of the watermark will be modified by this geometrical transformation increasing the error on the watermark extraction. As the watermark block will be extracted from the same location in the H matrix, it will contain some wrong values introduced by the change of the values position. For this reason, this method is more robust

against synchronous attacks than asynchronous ones presenting high degrees and levels of distortions. Using the Hessenberg domain, we can provide more robustness against different sets of intentional and malicious possible attacks. Various examples of these attacks are simulated below on the original cameraman image followed by the corresponding correlation values of the detected watermark block between 1000 other matrix blocks. For a robust watermark embedding only the fourth Hessenberg zone is used. We can embed in the other zones for a fragile watermark embedding method using a low gain factor to avoid damaging the image quality. In addition the image appearance can be changed by modifying the Hessenberg blocks matrix with respect to the zone location.

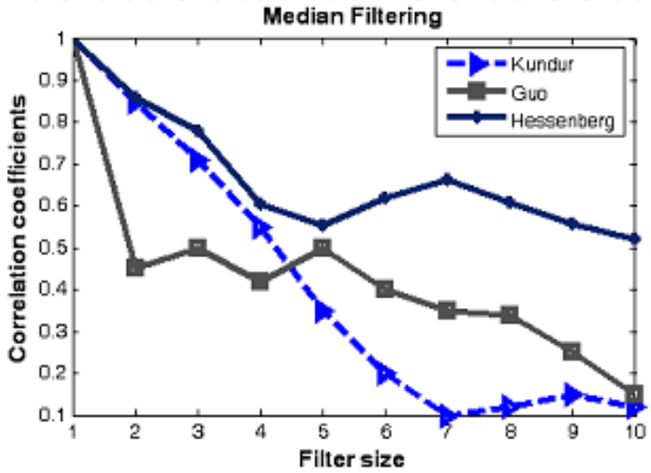


Fig. 19. Robustness against Median Filtering.

2.4.1 Experiment 1: Convolution filtering 1 and 2 attacks

Figures 20a, 20b, 21a, and 21b show applied convolution filters attack and the responses of the watermark detector to 1000 random blocks of the watermarked Hessenberg image matrix. The positive response due to the correct watermark block is much stronger than with incorrect blocks. The detection rates of these attacks are very high when compared

Fig. 20. a) Convolution 1 attack.

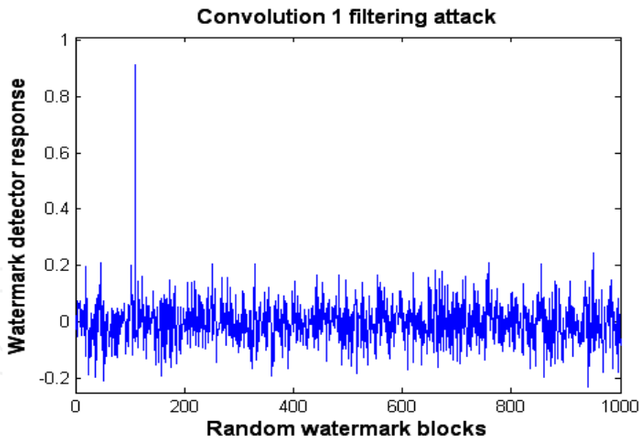


Fig. 20. b) Watermark detection result.

Fig. 21. a) Convolution 2 attack.

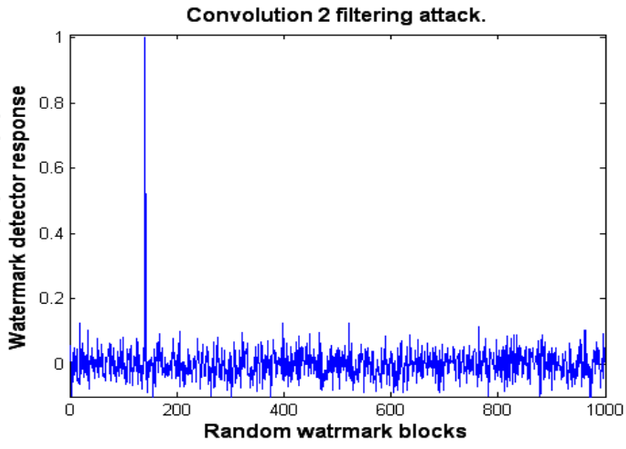


Fig. 21. b) Watermark detection result.

with other watermarking domains, such as the spatial domain [8]. Two filtering attacks are proposed: the convolution 1 and 2 filters, where the first represents a gaussian filter and the

second a sharpening filters. The parameters of the filters applied on the cameraman image as shown in Fig.20a and Fig.21a, is given as the following: CONV 1 filter = 3, 3, 9. Where the two first numbers corresponds to the filter width and high and the third number is the division factor. The matrix filter is $\begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix}$. The parameters of CONV 2 filter are the same, and its matrix is: $\begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix}$.

2.4.2 Experiment 2: JPEG compression attacks

Figures 22a and 22b show the results obtained after respectively applying a JPEG 20 and JPEG 60 compression on the image. This technique is found to be robust against this kind of signal processing distortion. A series of different JPEG compression rates are applied, as shown in Table 1, with high rates of watermark block detection. Using this method, the watermarked images are safe face to these unintentional signal processing attacks and the watermark can be entirely get back after this lossy compression.

Fig. 22. a) JPEG 20-compression attack.

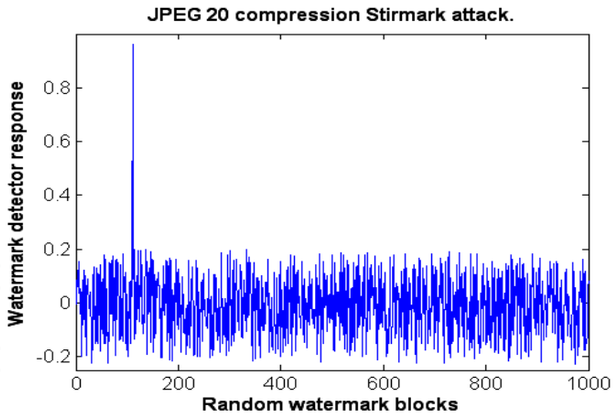


Fig. 23. b) Watermark detection result.

2.4.3 Experiment 4: Noise attacks

Gaussian noise with zero mean and varied variances σ .Different noise magnitudes are added to the watermarked image from (0 to 80), as shown in Table 1, with the corresponding watermark detector responses. In all the cases, the watermark was not removed, and the correlations with the real watermark block were higher. Figures 23a and 23b illustrate two noise attacks (80), with the corresponding normalized watermark detector responses.

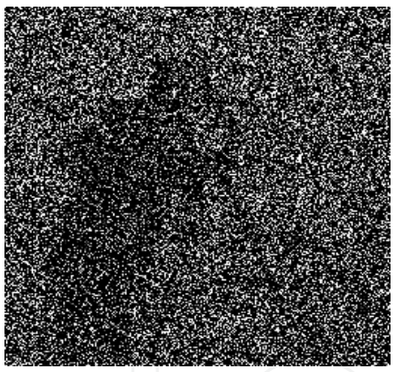


Fig. 23. a) NOISE 80 attack.

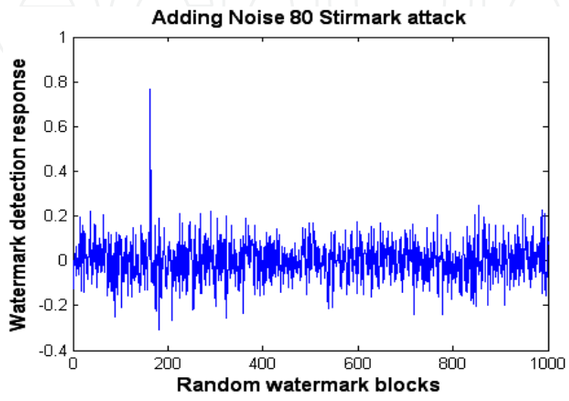


Fig. 23. b) Watermark detection result.

2.4.4 Experiment 5: Geometrical distortions

Different geometrical distortions are applied as attacks to the watermarked image such as rotations and affine transforms. The rotation attacks change the position of the image pixels and break the correlation between the image and the embedded watermark. Many rotation degrees are applied between which three are showed in the table above: two, forty-five and ninety degrees rotations attacks. The second kind of geometrical distortions attacks are the affine transform. Two kinds of affine attacks are applied indexed as affine 5 and affine 7.This geometrical transform is given by the equation (14).

$$\begin{vmatrix} X' \\ Y' \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \cdot \begin{vmatrix} X \\ Y \end{vmatrix} + \begin{vmatrix} d \\ e \end{vmatrix} \tag{20}$$

The variables a, b, c, d, e changes with the affine transform index and fixed by the Stirmark tool.

The proposed technique is found to be robust against this kind of signal processing distortion as shown by the correlation results in the table 1. Figures 24a and 25b show the response value of the watermark detection corresponding to the computed correlation between the original watermark block and the detected one after the applied attack, and the attacked watermarked image, respectively. The watermark block resists this image processing with a high correlation value, compared with the other matrix blocks used in the test.

Fig. 24. a) Affine 7 transform attack.

2.4.5 Effect of changing blocks in different Hessenberg matrix zones

As detailed in section 2, the Hessenberg matrix is divided in different zones. The choice of the zone in which the watermark block is substituted, is very important in order to avoid a possible image characteristics and appearance change. In this section, the influence of each matrix zone is illustrated. The fourth zone, which is indifferent with regard to the image quality when a watermark is embedded in, is also shown, and different images are

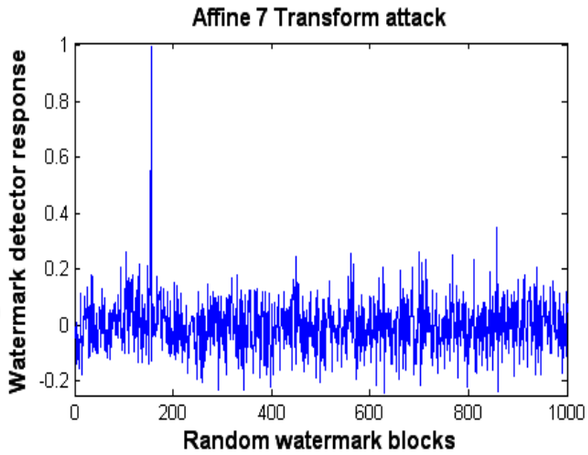


Fig. 24. b) Watermark detection result.

watermarked with various gain factors. All figures belonging to these simulations are detailed below in different sets. In all the sets of figures, the limits of the blocks processed are presented by [lines-limits, Columns-limits], and K represents the gain factor used.

Figures 25: "Image BLOOD", 26: "Image DOOR" and 27: "Image RICE" are the original images used throughout the simulation experiments, in addition to the "Cameraman" image shown in section 3. The images, from 28a to 28h, illustrate the results of changing blocks in the first zone applied to the "cameraman, door and blood" images with different gain factors, varying from 5 up to 35. The examples show the effect of operating in different sectors of zone 1. The damage caused to these images by changing blocks in this first zone results in local or general variable image blurring. In the set of figures, from 29a to 29f, the second zone of the transformed image matrix is changed. The simulation is applied to the different used images with different gain factors, as shown below. When changing a sector belonging to this zone, a string effect appears locally or on the entire image. The intensity of this string effect varies with the level's value of the gain used. Figures from 30a to 30i represent the results of simulations where the third zone is processed. In fact, this is an interesting zone. The result of changing blocks in zone 3 is shown in Figures 30a, 30b, 30c, 30d and 30g. Embedding a watermark in this zone affects these images by adding a non-uniform noise appearance. The intensity of this noise varies from one image region to another. Figures 30e, 30f, 30h and 30i show the effect of a uniformly distributed noise by changing the sectors detailed with the images.

In all these simulations, dealing with the fourth zone is the most interesting in this proposed Hessenberg watermarking method. From Figures 31a to 31i, the fourth zone of the transformed image matrix is changed. In fact, as we will detail in these figures, it is clear that this zone is the least sensitive to watermark embedding, and can be totally insensitive in some cases to the blocks changing. Figures 31a, 31b, 31c and 31d clearly show that changing the blocks in the fourth Hessenberg matrix zone does not affect the image quality where no visible changes are observed in the watermarked image even though the gain increases from 1 up to 35. As shown in Figure 31e when using the "Cameraman" image, some visible changes begin to appear in the upper left corner of the watermarked image as indicated by the arrow if the applied gain factor reaches the value 38. The same distortions are shown in Figure 31f, with a gain factor that reaches 50. In the figure 31g, the same gain factors is used, and the same block is changed, we note no visible changes appear in the watermarked

"Blood" image. Some other images require higher gain factors to be affected by certain changes. Figures 31h and 31i show the "Door" and "Rice" images, where a gain factor of 210 and 250 respectively, is applied. Until the gain factor reaches these high values, some visible changes begin to appear, as indicated by the arrows on the regions affected by the changes. It is clear that the gain factor used, and which is capable of causing some damage or changes to the watermarked image differs with the image type and characteristics. Of course, using a high gain factor implies higher correlation values and watermark detection between the attacked watermarked image and the original one. The Table 5 presents the different PSNR corresponding to the figures from 31a to 31i. The computed PSNR shows the distortion magnitude introduced to these test images watermarked in the fourth Hessenberg zone.

Figures number	21a	21b	21c	21d	21e	21f	21g	21h	21i
PSNR (dB)	44.72	44.68	44.60	49.70	44.41	44.32	49.65	42.72	43.12

Table 5. PSNR variation against different watermarked test images with variable embedding strength.

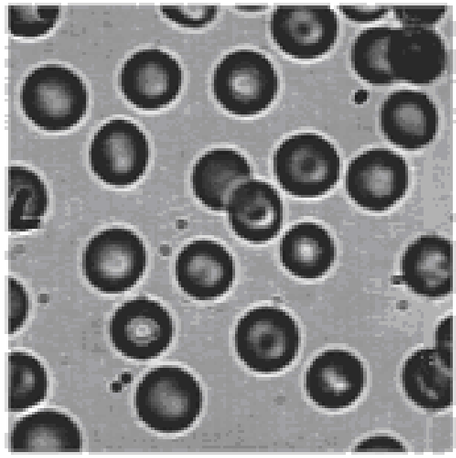


Fig. 25. Original image “Blood”.

Fig. 26. Original image “Door”.

Original image “Rice”.

Fig. 27. The original images used in the simulations.

Fig. 28. a) [1:10,10:20], K = 5.

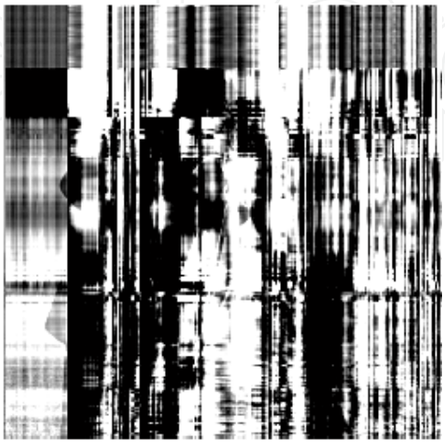


Fig. 28. b) [1:10,10:20], K=20.

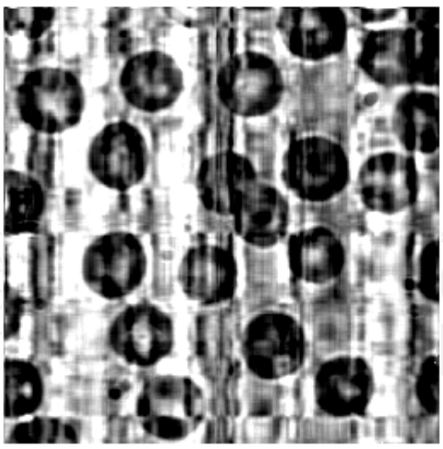


Fig. 28. c) [1:10,10:20], K=5 (Blood).

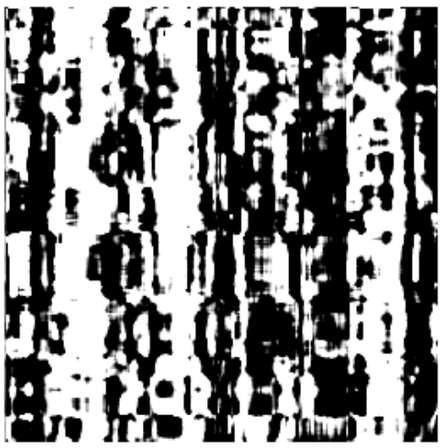


Fig. 28. d) [1:10,10:20], K=35 (Blood).

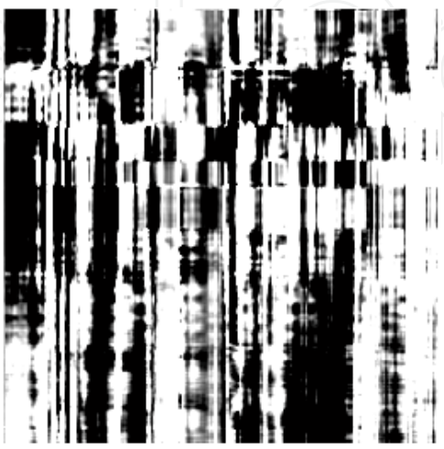


Fig. 28. e) [1:10,10:20], K=20 (door).

Fig. 28. f) [1:10, 50:100], K=5.

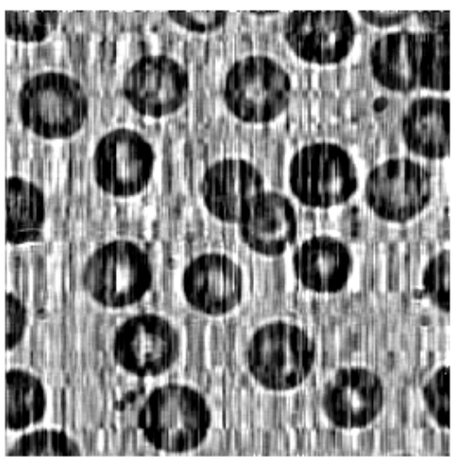


Fig. 28. g) [1:10, 50:100], K=5 (blood

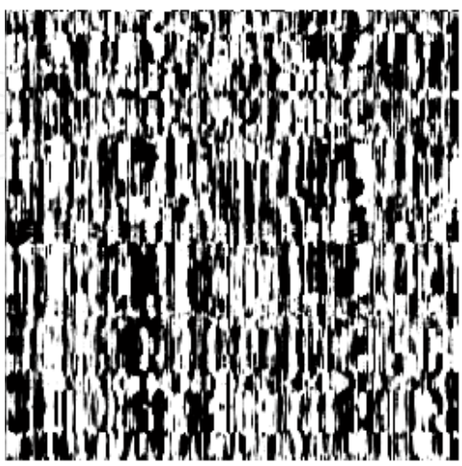


Fig. 28. h) [1:10, 50:100], K=35.
Fig. 28. Result of changing blocks in the first zone on the image.

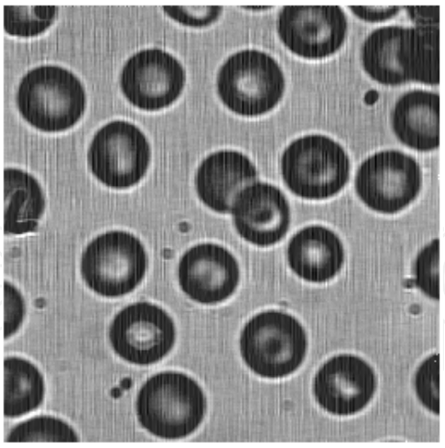


Fig. 29. a) [1:10,230:256], K=5.

Fig. 29. b) [1:10,230:256], K=5.

Fig. 29. c) [1:10,230:256], K=20.

Fig. 29. d) [1:10,230:256], K=20.

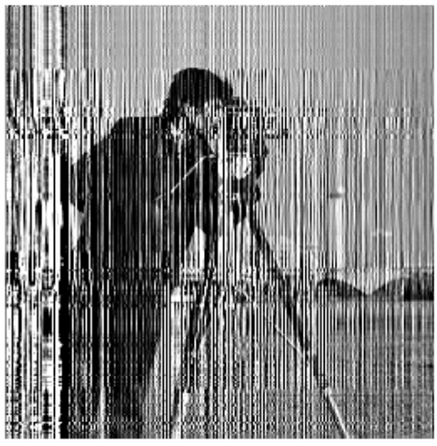


Fig. 29. e) [1:10,230:256], K=35.

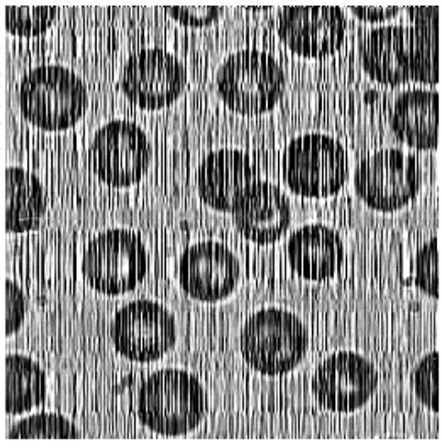


Fig. 29. f) [1:10,230:256], K=35.
Fig. 29. Result of changing blocks in the second zone on the image.

Fig. 30. a) [30:60, 60:100], K=5.

Fig. 30. b) [30:60,60:100], K=25.

Fig. 30. c) [30:60,150:256] K=5.

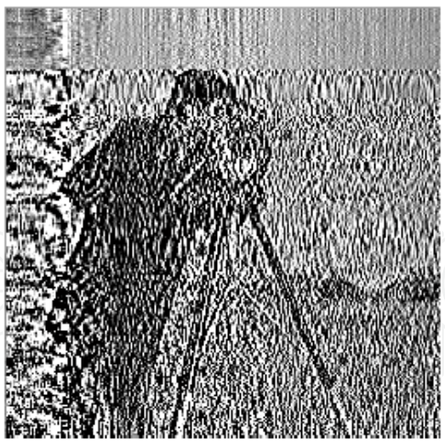


Fig. 30. d) [30:60,150:256], K=35

Fig. 30. e) [100:180,100:180], K=5.

Fig. 30. f) [100:180,100:180], K=20.

Fig. 30. g) [100:180,100:180], K=20.

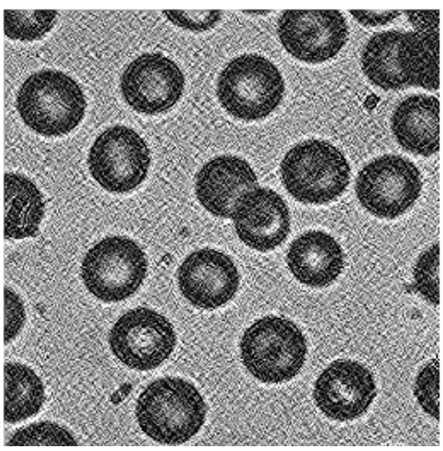


Fig. 30. h) [100:180,100:180], K=35

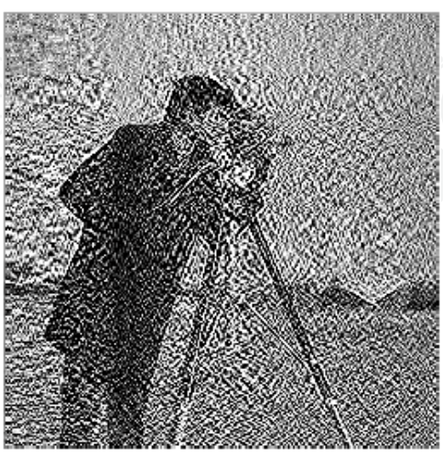


Fig. 30. i) [100:180,100:180], K=35.
Fig. 30. Results of changing blocks in the third zone on the image.

Fig. 31. a) K=5.

Fig. 31. b) K=10.

Fig. 31. c) K=20.

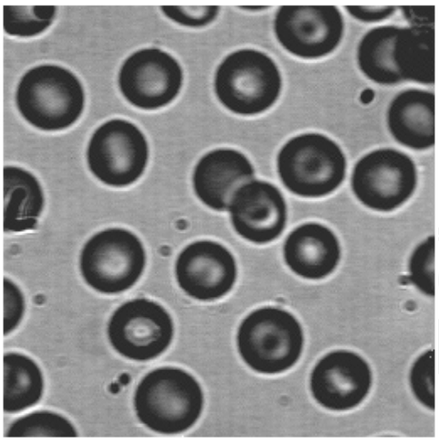


Fig. 31. d) K=35.

Fig. 31. e) K=38.

Fig. 31. f) K=50.

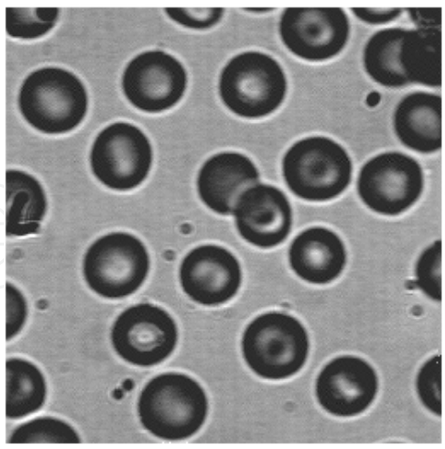


Fig. 31. g) K=50.

Fig. 31. h) K=210.

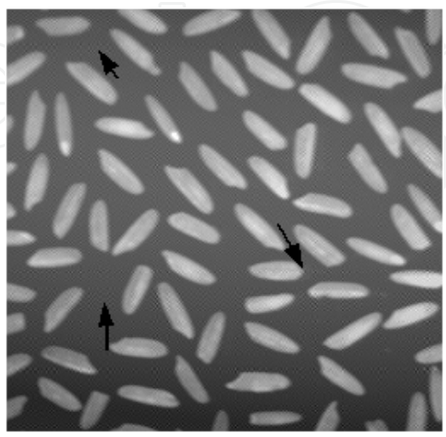


Fig. 31. i) K=250.
Fig. 31. Result of changing blocks in the fourth zone on the image.

4. A new watermarking method using the parametric hough transform domain

4.1 Introduction

Different constraints are required in a watermarking method, such imperceptibility and robustness. Besides, lossy JPEG compression remains the most unintended used attacks with data exchange in Internet, for size reduction. It can seriously affect the embedded watermark if the compression rate is high and the used scheme presents a weakness against this attack. So, the best solution resides in exploiting the DCT domain used in the JPEG algorithm in order to dispose of the robustness against this compression or the multi-resolution domain as in. But acting to be robust against this attack reveals automatically the domains of watermark embedding and than increase the possibility of its detection. In this section, a novel watermarking method is proposed. It consists in using the parametric space of the mathematical Hough transform as a watermarking domain. The technique consists in selecting specific maximums in the Hough matrix with respect to a secret key. The peaks are found to be invariant points in the proposed Hough domain especially against lossy JPEG compression. Two signatures are considered; the first is hold in the Hough domain by the transformed space and consists in the locations of the specific chosen invariant points. Whereas, the second is represented by the use of end points of the correspondent detected lines. These end points are used as centers to embed similarities blocks in. The watermarking in this domain is found to be extremely robust against JPEG compression and some geometrical transforms. All these attacks are generated by the STIRMARK tools. This section is organized as the following: In section 2, an overview of the Hough transform is presented. Section 3 details the proposed method in the Hough domains: the carried study and the proposed solutions. In section 4, we study the robustness of this technique against different STIRMARK attacks by testing its capacity to detect the embedded watermark. The privileges offered by this approach are also detailed, and finally we conclude this work.

4.2 Hough transform overview

The Hough transform is a mathematical algorithm used in images processing to detect the presence of parametric forms as ellipses or lines in the image. This technique uses the principle of evidences accumulating to prove the existence of a particular form in the image. For this aim, this transform uses a parametric domain or space to characterize these forms. Each form is represented by its proper parameters in this space. In our work, this transform is coded to be used as lines detector where its parametric space is exploited. It's important to note that the Hough transform is found to have the capacity to detect the same segments or broken lines in the image, before and after being compressed. This detection invariance is due to the fact of the invariance properties of its parametric space in the case where the image is subjected to JPEG compression and some asynchronous transforms. In the case of lines detecting, the Hough transform is presented as follows:

Each line can be described in the orthonormal space by the equation (1) or (2)

$$y = a \,.\, x + b \tag{1}$$

$$\rho = x \cdot \sin\theta + y \cdot \cos\theta \tag{2}$$

The parametric space is than composed by two parameters: ρ and θ that forme a space matrix as shown in figure 1.

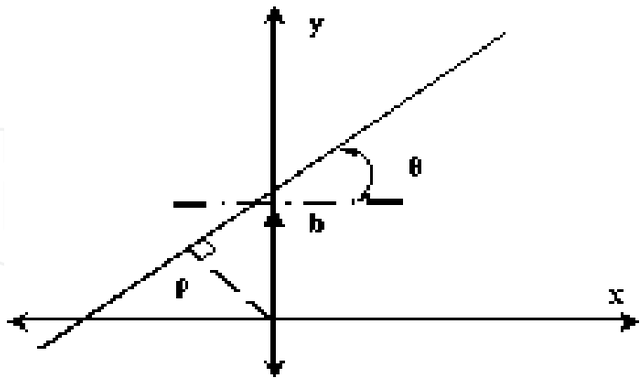


Fig. 1. The parametric space (ρ, θ).

An infinity of lines can pass through a fixed point called P having (x,y) as coordonates. But if we consider a second point P_1 having (x1,y1) as coordinates, only one line can pass through P and P_1 satisfying the same couple of (ρ and θ). If this principle is applied to the image, the Hough transform of an image generates a parametric space matrix as presented in (3):

$$H\left(M\right) = \mathrm{A}\left(\rho, \theta\right) \tag{3}$$

Where H is the Hough transform, M is the image matrix and A is the space parametric resulting matrix. Since this matrix contains a limited number of elements, the number of possible detected lines is with respect to the quantization step of ρ and θ in their respective variation domains. Peaks contained in this space represent an accumulation of evidences indicating the possibility of lines presence with respect to a specific position and orientation.

4.3 The proposed method

In this work, we propose to apply the philosophy of the Hough transform on the image in order to process and manipulate it in the parametric Hough space, and use it as a watermark-embedding domain. If we consider an (N×M) image; in order to accumulate evidences and define the parametric space, the information source is gathered from the pixels composing the image. More the evidences are accumulated and put in the parametric space matrix; more the chance to identify a real line in the image is high. In the following, we will define the parametric space matrix generated by the Hough transform as the Hough space or Hough domain. The first step consists in applying a high pass filter in order to extract the image edges. In each point belonging to this edge, infinity of lines can pass through it. Accumulating evidences in the parametric space provides the unique position and orientation (ρ and θ) for witch one line can pass through this point. In our case the positions and the orientations are quantified by a step computed with respect to the required precision. The Hough space is than a two-dimensional matrix or map. The size of this map depends on the quantification step as shown in Figure 2.

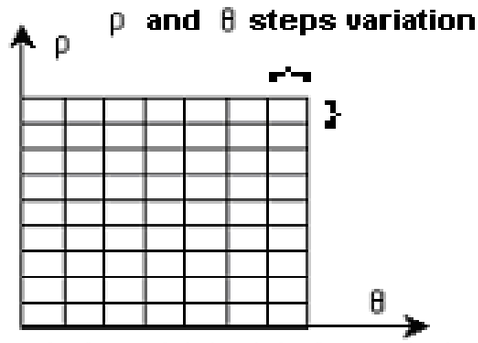


Fig. 2. The parametric space map.

The quantification steps are computed as follow:

Consider an image with size N×M, θ can vary in the interval range of [0, 2π], the value of ρ is maximum when it's computed in the image diagonal. The steps and variation domains of ρ are than described by the equations (4, 5, 6 and 7):

$$\rho_{MAX}^2 = \left(\frac{N}{2}\right)^2 + \left(\frac{M}{2}\right)^2 = \frac{\sqrt{N^2 + M^2}}{2} \tag{4}$$

$$\rho_{MAX} \in \left[0\,,\ \frac{\sqrt{N^2 + M^2}}{2}\right] \tag{5}$$

More the quantification steps are decreased, better the resolution is; but the Hough matrix size increase. In order to attend equilibrium between: resolution, computing time and parametric space dimension, we will fix the orientation step depending on the image size. If θ varies as

$$\theta \in \left[0\,,\ \frac{2\pi}{\sqrt{N \cdot M}}\right] \tag{6}$$

If the image is square the resolution will be as:

$$\theta \in \left[0\,,\ \frac{2\pi}{N}\right]; \text{and } \rho_{MAX} = \frac{\sqrt{2}}{2} \cdot N;\ with\ \Delta\rho = \sqrt{2} \tag{7}$$

In the following, we will consider the ρ step as:

$$\Delta\rho = \frac{\rho_{MAX}}{100} \tag{8}$$

$$\Delta\rho = \frac{\sqrt{N^2 + M^2}}{200} \tag{9}$$

These steps provide an acceptable precision to browse the entire image as shown in Figure 3.

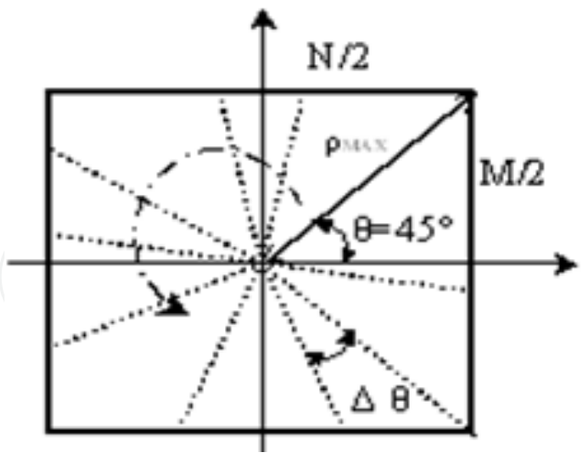


Fig. 3. Image browsed by ρ and θ variation.

The operation of accumulating evidences in the Hough matrix for potential presence of lines in the image is characterized by the appearance of maximums in the matrix. A threshold is previously chosen to characterize since witch values we can consider maximums in the space parametric matrix as peaks. The number of picks and their position in the Hough map is used as secret key. By finding and fixing the peaks number, we extract the correspondent lines and respectively their end points. These end points are used as centres of blocks similarities embedding. In fact in each end point we extract a block of size $(2n+1) \times (2n+1)$. All these blocks are substituted with similarities as shown by the equations (10) and (11). If we consider B_i as the chosen block, W_i the watermark and B_{wi} the watermarked block:

$$W_i = \text{dyn}\left(B_i\right) = \frac{B_i - \ddot{\ddot{B}}_i}{\max\left(B_i - \ddot{\ddot{B}}_i\right)} \tag{10}$$

$$B_{wi} = B_i \cdot \left(1 + \alpha \cdot W_i\right) \tag{11}$$

Where $\ddot{\ddot{B}}_i$ is the indexed block mean and α is the watermark embedding strength. In the experimental results, as will be shown in the next section, the selected peaks (maximums) in the Hough space matrix corresponds to the embedded watermark location in the image. The peaks position in the Hough space and their respective end points in the spatial representation, are completely invariant when the image is attacked by JPEG compression or some geometrical transforms.

4.4 Experimental configuration

In our experiments, the cameraman image is used to simulate the applied method and the chosen attacks. This image is chosen because of its content variation. In fact it contains lines in addition to homogeneous and textured zones. A binarizing method is applied to convert

this image into a binary image. An edge extractor filter is then applied to extract the image edges. Once theses edges are taken out, the Hough transform is coded and then applied on the resultant image to browse it and then accumulates evidences in the transformed parametric matrix to decide witch maximums corresponds to real lines in the image. In this matrix, the number of chosen peaks and their respective position represents the secret key used to select the ends of the correspondent lines where the similarities blocks are embedded. The position of the peaks are returned and saved to be compared with the same peaks position after the attacks are applied on the image and view if they can be considered as unvaried points with respect to the applied attack. The peaks are defined as the entire matrix maximum that exceeds a fixed threshold. In this work, in order to obtain a better precision, the threshold is fixed as $T_h = 0.7$ and then:

$$P_K = T_h \cdot \max(H) \tag{12}$$

Where P_k represents the returned peaks, H is the Hough matrix. Different peaks can be selected and then view theirs corresponding lines and end points in the image as shown in Figures 4, 5, 6 and 7.

4.5 Simulation results

In the following, the number of peaks is chosen equal to one. The location of the peaks in the Hough parametric space is represented by the respective position in the matrix lines and columns as (L, C).

The first peak is selected and its position is returned as (-23, 89.2472) in the Hough matrix space. That means that $\theta = -23°$ and $\rho = 89.2472$. Figures from 8 to 11 present the detected peaks in the Hough space and their respective positions shown in Table 1. The correspondent detected lines and respectively their end points where the similarities blocks are embedded are shown in these figures. The Table 1 presents the attacks applied on the cameraman image; the JPEG compression and the rot-scale transform. The extracted peaks after the attacks have been applied presented. A total invariance is remarked concerning the peaks positions against lossy JPEG compression.

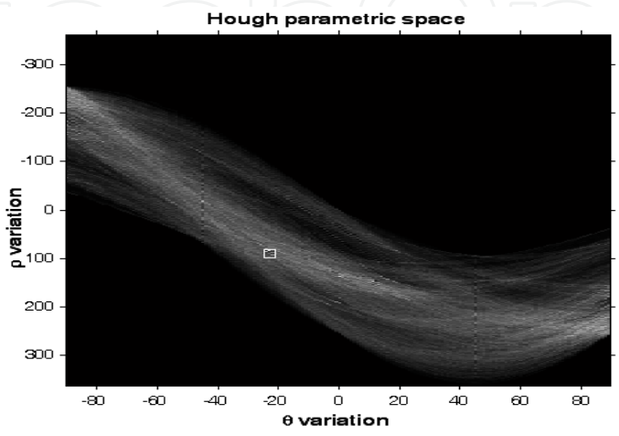


Fig. 4. The first pick in the parametric Hough space.

Fig. 5. Three detected segments corresponding to the first selected peak presented in Fig.4.

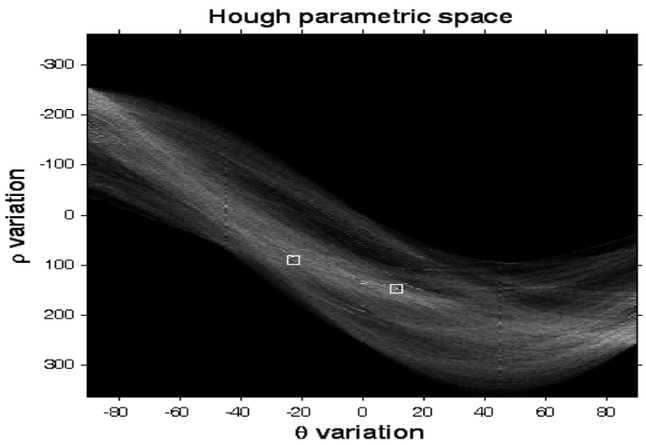


Fig. 6. Two first picks in the parametric Hough space.

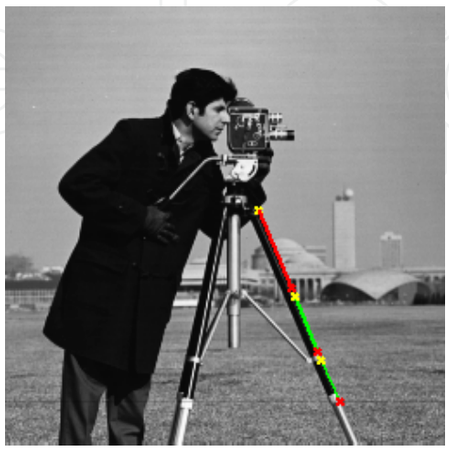


Fig. 7. Detected segments corresponding to the first selected peak presented in fig.6.

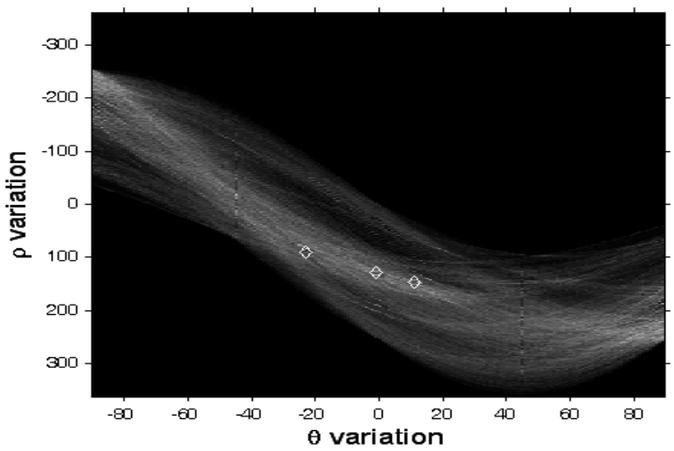


Fig. 8. The three first selected picks.

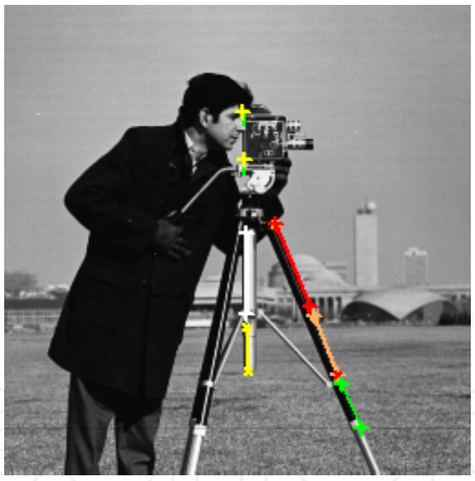


Fig. 9. Detected segments corresponding to the three first selected peaks presented in Fig.8

4.5.1 Experiment 1: JPEG compression

The figures from 8 to 11 show respectively the cameraman image attacked by the JPEG 10, 20 and 40 compression and the obtained result of the detected peaks position leading to the watermark detection. The proposed method based on the Hough parametric space is found to be highly robust against lossy compression. A series of different JPEG compression rates from JPEG 100 to JPEG 10 are applied as shown in Table 1. The distortion caused to the watermarked image by all these attacks hasn't changed the position of the selected peaks in the Hough space.

APPLIED ATTACK	PEAK POSITION IN THE HOUGH SPACE
JPEG 100	(-23, 89.2472)
JPEG 90	(-23, 89.2472)
JPEG 80	(-23, 89.2472)
JPEG 70	(-23, 89.2472)
JPEG 60	(-23, 89.2472)
JPEG 40	(-23, 89.2472)
JPEG 30	(-23, 89.2472)
JPEG 20	(-23, 89.2472)
JPEG 10	(-23, 89.2472)
ROTSCALE –0.25	(-23, 89.2472)
ROTSCALE –0.5	(-23, 89.2472)
PSNR 100	(-23, 89.2472)

Table 1. Invariance of the selected peak position against applied attacks.

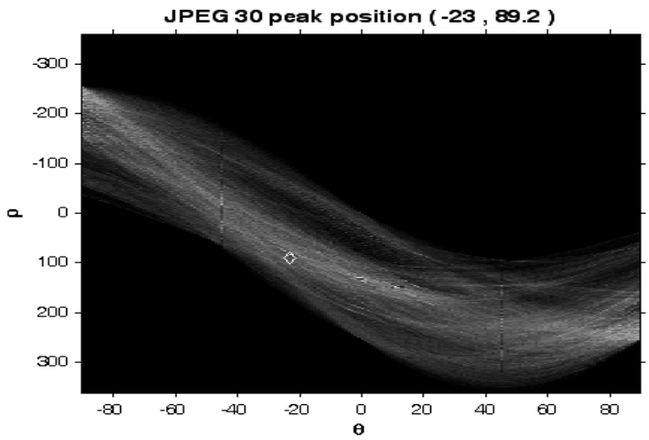


Fig. 10. The position of the detected peak in the JPEG 30 compressed image.

Fig. 11. End points of the detected lines correspondent to the peak in Fig.10.

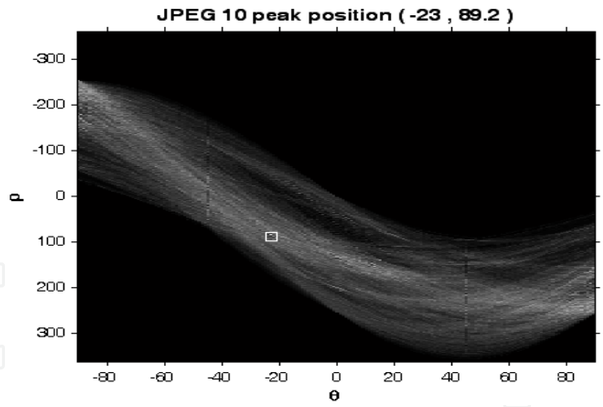


Fig. 12. The position of the detected peak in the JPEG 10 compressed image.

Fig. 13. End points of the detected lines correspondent to the peak in Fig.12.

4.5.2 Experiment 2: Asynchronous attacks

Figures 14 and 16 show the rotation and scale attack, and the correspondent detected peaks position in the Hough space. As shown in the Table 1 and the figures below. The use of this space provides high robustness against these attacks and grant invariance properties to the selected peaks if the image is attacked, especially when dealing with small distortions the invariance of the peaks position is kept unchanged.

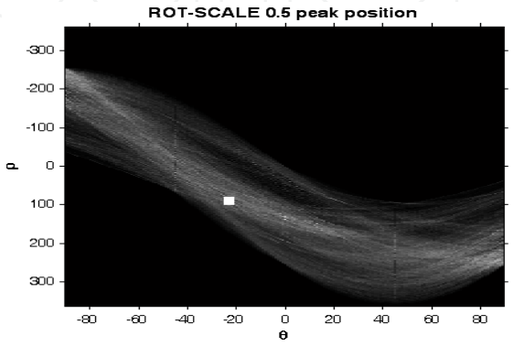


Fig. 14. The position of the detected peak in the ROT-SCALE 0.5 attacked image.

4.6 Evaluation and comments

In this section, we comment the results and compare our proposed methods to other ones. As shown previously, this method is highly robust against JPEG compression. The Peaks positions are unvaried whatever the compression rate used. The image is represented by the Hough parametric space as a new representation domain where the signature is characterized by the unvaried positions of the selected peaks and hold in it. The robustness of this method is picked out from the robustness of this new Hough domain face to JPEG and other attacks. In fact, the parametric Hough space holding the signature cannot be modified by synchronous attacks as JPEG, filtering, i.e. it doesn't modify the pixels position and then the ends of lines. As a result, the detected peaks after the Hough transform is applied remain unvaried. Conversely, the asynchronous attacks that modify vastly the pixels position change the position of the lines ends and then modify the positions of the Hough space peaks. Figures 16 and 17 show the asynchronous rot-scale attack with two degrees and the correspondent detected peaks.

Fig. 15. End points of the detected lines correspondent to the peak in Fig.14.

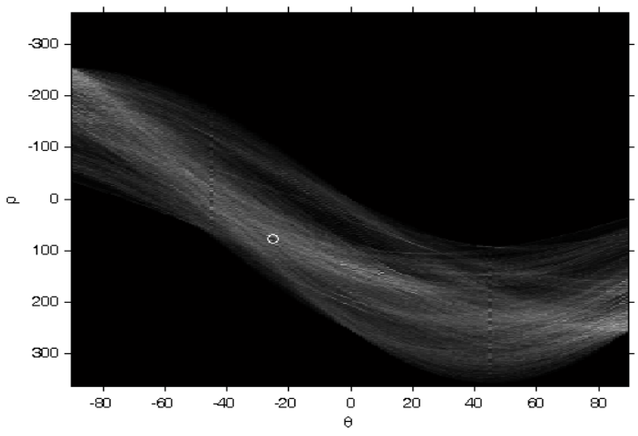


Fig. 16. Rot_scale 2° peak position.

Fig. 17. Peaks detected corresponding to Fig.16.

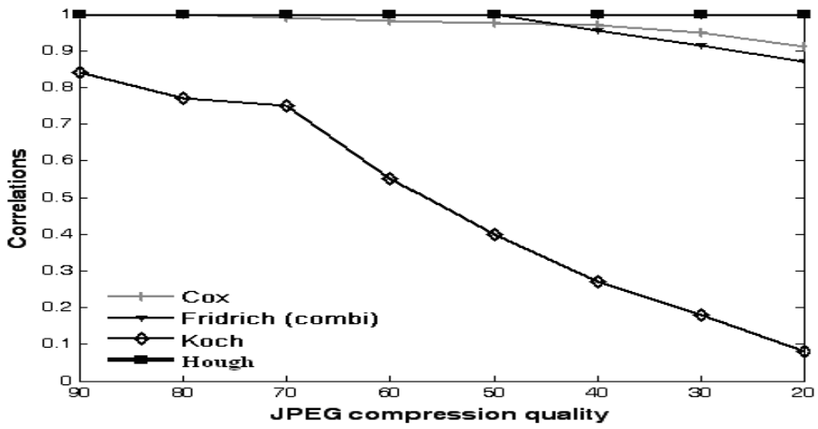


Fig. 18. Robustness of the Hough algorithms.

Figure 18 shows the robustness of the proposed Hough algorithm when compared with the well known and most robust algorithms proposed in the DCT domain to defeat the JPEG compression attacks. It's evident that our algorithm is the most robust. This method is found to be better than those actually in use, due to the fact that the image is not processed similarly to the methods in use that embed the watermark by modifying the image either in the spatial domain or in the frequency and multi-resolution domains.

5. Conclusion

A new domain and watermarking techniques are proposed in this work. In the first presented approach, sing the mathematical Hessenberg transformation, the original image is transformed in the Hessenberg domain as a triangular matrix which values present specific characteristics. The embedding procedure is applied to a transformed image in a non-sensitive zone that has no effect on the image quality after an inverse transformation is applied. Processing the lowest values in the entire matrix, by modifying them we impose a low variation on the original coefficients of the image and no distortions appears on the watermarked image. A study was carried out to show how the Hessenberg matrix can be

partitioned, and the effect of each matrix zone on the image perception. Many advantages are proposed by the use of this method. In fact it allows the use of a high embedding strength which allows being more robust against attacks than DCT, DFT or spatial methods. Its robustness against lossy JPEG compression exceeds this allowed by the well known and used until now DCT domain. In addition, by choosing the appropriate zone and changing some of its values, this technique is able to give the appearance of a noised, banded or blurred image without really applying these signal processing operations on the image. This technique is found to be very resistant against simultaneous a large set of synchronous and asynchronous signal processing attacks, and the watermark is always present in the entire set of the attacked image. The watermark detection process and the similarities computing presented in this approach are obtained from tests applied on the "Cameraman" image with a gain factor of 35. Evidently, the embedding strength can be highly augmented without exceeding the watermark imperceptibility when dealing with certain kinds of other images presenting different characteristics that allow high gains value without any changes, as shown in Figures 31h and 31i. Markedly, this high gain increases the robustness of the embedded watermark and improves vastly the results of the proposed method. We finally note that we propose a blind watermarking technique; the presence of the host image is not required for watermark detection procedure.

In the second approach, a new watermarking method is presented. Based on the mathematical hough transform, a parametric space matrix is obtained and used as a new space where the image is processed. A secret key is characterized by the number of selected peaks in this space matrix is chosen. These peaks are found to be invariant and robust against jpeg compression and some asynchronous transforms. They are also used to determine the correspondent lines end points where similarities blocks are embedded. The embedded watermark is carried in hough space by the invariant peaks and their position that corresponds to the embedded similarities. This method proposes higher resistance against lossy compression than the previous algorithms based essentially in the DCT domain.

6. References

E. Anderson, Z. Bai, C. Bischof, S. Blackford, J. Demmel, J. Dongarra, J. Du Croz, A. Greenbaum, S. Hammarling, A. McKenney, and D. Sorensen, “LAPACK User's Guide”, Third Edition, SIAM, Philadelphia, 1999.

M. Barni, F. Bartolini, A. De Rosa and A. Piva, “ Capacity of the watermark channel: how many bits can be hidden within a digital image”, Proc. SPIE 3657, 1999, pp. 437-448.

P. Bas, J.M. Chassery and B. Macq, “Image watermarking: an evolution to content-based approaches”, Pattern Recognition 35 (2002), pp.545-561.

P. Bas and J.M. Chassery, Tatouage d’image résistant aux transformées géométriques, 17éme colloque GRETSI, Vannes, France, 13-17 Septembre 1999.

G. Caronni, “Assuring ownership rights for digital images”, Proceeding of reliable IT Systems, VIS' 95, Viewveg Publishing Company, Germany, 1995.

L. Chang, “Issues in Information Hiding Transform Techniques”, Storming Media, Computers: Cybernetics, 20 May, 2002, http://www.stormingmedia.us/84/8491/A849104.html.

L.H. Chen and J.J. Lin, "Mean quantization based image watermarking", Image and vision computing vol. 21, No. 8, 1 August 2003, pp. 717-727.

P. Chun Chen, Y. Sheng Chen, and W. Hsing Hsu, "A communication system model for digital image watermarking problems", International conference on Information Systems Analysis and Synthesis , ISAS, Vol.6, pages 2935, USA,1999.

I. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Process. No. 6, Vol. 12, June 1997, pp.1673-1687.

F. Davoine and S. Pateux, "Tatouage de documents audiovisuels numériques", Hermes science, Lavoisier 2004.

L.Diane, Cours de traitement d'images, Laboratoire I3S Informatique, Signaux et Systèmes, Université de Nice Sophia Antipolice, Rapport de recherche ISRN I3S/ RR, 22 janvier 2005.

A. Fabien, P. Peticolas, "Watermarking schemes evaluation", IEEE Signal Processing Magazine, Vol. 17, no. 5, pp. 58-64, September 2000.

A. Fabien, P. Petitcolas, M. Steinebach, F. Raynal, J. Dittmann, C. Fontaine and N. Fatès, "A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark", In Ping Wah Wong and Edward J. Delp, editors, proceedings of electronic imaging, security and watermarking of multimedia contents III, vol. 4314, San Jose, California, U.S.A., 20-26 January 2001.

J. Fridrich, Combining low-frequency and spread spectrum watermarking, In Proceedings of the SPIE Symposium on Optical Science, Engineering and Instrumentation, San Diego, USA, July 1998.

G. H. Golub, and C. F. Van Loan, "Matrix Computation", Johns Hopkins University Press, 1983, pp. 384.

M. Van.droo. Genbroeck, "Acquisition et traitement d'image", Université de Liège publication, Institut Montefiori, Service de télécommunication et d'imagerie, Septembre 2001, version 4.14.

H. Guo and N. D. Georganas, "Multi-resolution Image Watermarking Scheme in the Spectrum Domain", IEEE Canadian conference on electrical and computer engineering, pp125, may 2002.

F. Hartung and M. Kutter, Multimedia watermarking techniques, Proc. IEEE Vol. 87, No. 7, 1999, pp. 1079-1107.

J. Huang, Yun Q. Shi and Yi Shi, "Embedding image watermarks in DC components", IEEE Trans. Consumer Electron. 46 3 (2000), pp. 415-421.

N. Kaewakamnerd and K.R. Rao, Wavelet based image adaptive scheme, Electronics letters Vol. 36, 2000, pp. 312-313.

S. Katzenbeisser, F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech house, December 1999.

E. Koch and J. Zhao, Towards robust and hidden image copyright labeling, Proceedings of the IEEE International Workshop on Nonlinear Signal and Image Processing, pp. 452-455, Halkidiki, Marmaras, Greece, June 1995.

X .Kong, Y. Liu, H. Liu and D. Yang, "Object watermark for digital image and video", Image and vision computing journal, Vol.22, Issue.8, August 2004, pp. 583-595.

D. Kundur and D. Hatzinakos, "Diversity and Attack Characterization for Improved Robust Watermarking", IEEE Transactions on Signal Processing, Vol. 49, no. 10, Oct 2001.

P. Lan, "Robust transparent image watermarking system with spatial mechanisms", Journal of systems and software, 15 February 2000, 107-116.

G.C. Langelaar, I. Setyawan, and R.L. Lagendijk, "Watermarking in digital image and data: A state of the art overview", IEEE Signal Processing magazine, September (2000), pp. 20-40.

M. Laug, "Traitement optique du signal et des images", Ecole Nationale Supérieure de l'Aéronautique et de l'Espace SUP'AERO, Edition Cépaduès, France, 1980.

P. Moulin, M.K. Mihcak, "A framework for evaluating the data-hiding capacity of image sources", IEEE Transactions on Image Processing, September 2002, vol. 11, no. 9, pp. 1029-1042.

A. Natarajan, "Discrete cosine transform", IEEE Trans. on Computers, 1974, Vol. c-23, pp 90-93.

N. Nikolaidis and I. Oitas, "Robust image watermarking in the spatial domain", Signal Processing, vol. 66, no. 3 (1998), pp. 385-403.

I. Pitas, T. Kaskalis, "Applying signatures on digital image", Workshop on Nonlinear Signal and Image Processing, IEEE, Neos Marmaras, June 1995, pp 460-463.

C.I. Podichuck and W. Zeng, image adaptive watermarking using visual models, IEEE journal on selected area in communication, Special Issue on Copyright and Privacy Protection, Vol. 16, 1998, pp. 525-538.

V. Rouilly, Présentation de la transformée de Hough, Rapport interne, ENST, Raris, France, http://www.tsi.enst.fr/tsi/enseignement/ressour ces/mti/ellipses/Hough.html .

J. O'Ruanaidh and T. Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Proc. IEEE international conference on image processing, Vol. 1, pp. 536-539, 1997.

K. Sayood, "Data compression", Maurgan Kaufmann Publishers, San Francisco, CA, 2000.

H. Seddik, M. Sayadi and F. Fnaiech, "A New Watermarking method using the parametric Hough Transform Domain", WSEAS Trans. on Information Science and Application, no. 9, Vol. 2, Sep. 2005, pp. 1277-1284.

H.Seddik, E.Ben.Braiek, "Color Medical Images Watermarking" ICGST International Journal on Graphics, Vision and Image Processing, Vol.6 Special Issue on Medical Image Processing, pp.81-86, March 2006.

J.S. Seo and C.D. Chang Yoo, Localized image watermarking based on features points of scale-space representation, Pattern Recognition, Vol. 37, No. 7, July 2004, pp. 1365-1375.

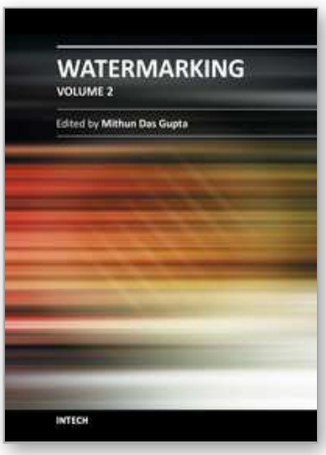
F.Y. Shih, S.Y.T. Wu, "Combinational image watermarking in the spatial and frequency domains", Pattern Recognition, vol. 36, Issue 4, April 2003, pp. 969-975.

P. Su, C.J. Kuo and H.M Wang, Blind digital watermarking for cartoon and map images, SPIE conference on security and watermarking of multimedia contents, San Jose, CA, USA, January 1999 pp. 296-305.

T.L. WANG and W.B. GRAGG, "Convergence of the shifted QR algorithm for unitary Hessenberg matrices", Mathematics of computation, Volume 71, Number 240, pp. 1473-1496,November 30, 2001.

R. Wolfgang, E. Delp, "A watermarking technique for digital imagery: further studies", International Conference on Imaging Science, Systems and Technology, Los Vegas, Nevada, July, 1997.

K.E. Zhao, "Embedding robust labels into images for copyright protection", Technical Report, Fraunhofer Institute for Computer Graphics, Darmatadt, Germany, 1994.



Watermarking - Volume 2

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0619-7
Hard cover, 276 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Hassen Seddik (2012). 2D Watermarking: Non Conventional Approaches, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-2/2d-watermarking-non-conventional-approaches

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen