ROBUSTNESS EVALUATION OF WATERMARKING BASED ON THE HARRIS PRINCIPLE

Maliki Badolo and Telesphore Tiendrebeogo

Department of Mathematics and Computer Science, Nazi Boni University, Bobo-Dioulasso, Burkina Faso

ABSTRACT

In the field of health, the messages conveyed by images have a considerable impact on the life of patients. In order to facilitate decision support on medical imaging, we will present in this paper the method of digital image watermarking based on the Harris principle whose objective is to hide the data in a medical image in order to evaluate its robustness. In addition, it ensures that the patient's image is authentic for a better diagnosis. To carry out this work we decided to start on the basis of two principles namely those of Moravec and Harris to obtain a solution that meets the need for digital watermarking. They consist in taking a random image (medical or not) and extract these points of interest and we obtain a mark, then take the original image of the patient that we add to the mark to obtain a digital image watermark. This watermark is invisible since all the invisibility properties are respected.

KEYWORDS

Watermark, Medical Images, Telemedicine, Harris, Stenography, Cryptography

1. INTRODUCTION

Since the beginning of the 20th century the Internet has been one of the most useful means of communication. In this era where the digital boom is in full swing, the issue of security is becoming a major concern in all areas. Particularly in the health field, there is a growing desire to be able to safely transfer a physician's medical record from one location to another, while at least ensuring the integrity and confidentiality of the content. This ensures that a medical image will not be intercepted by a malicious person [11]. Medical imaging plays an important and vital role in diagnosis support and decision-making [8, 5].

The objective of our paper is to propose a solution that will evaluate the robustness of a data hiding technique in a medical image. The principle of digital watermarking (invisible) [24] and [15] consists in inserting information in an image and to make it invisible to all people who is not entitled to see it. It allows to identify the owner thanks to an imperceptible signature and resistant to the attacks. According to [13] the inserted mark must however respect two fundamental constraints: the imperceptibility and the indelibility. It should be noted that the watermark is different from the other techniques of protection of document, because it is bound to the document and resistant. Therefore, the watermark is theoretically independent of the file format and it can be detected or extracted even if the document has been modified or if it is incomplete [24]. This method goes even further by guaranteeing the integrity of the image even after the reception of the image [3]. It should be noted that the digital image watermarking that we deal with in this document is mainly based on medical imaging and the Harris principle [1]. This method, inspired by the works of FOURATI and Bouhlel, Ali Hajjaji, Kumar Samir, and Samir Bandyopadhyay and William Puech [24, 15, 6, 9] interested us..

Our article starts with a state of the art which consists in presenting the various methods of digital image watermarking and the various techniques of attack of the digital image watermark. Then the methodology and the context of watermarking to finish with the expected results. Finally, the paper ends with a conclusion and perspectives.

2. RELATED WORK

Digital image watermarking, also known as digital image watermarking, has been very successful in the world, especially in the health sector (telemedicine). However, researchers continue to find ways to improve existing solutions. It should be noted that several solutions were brought in the case of the medical image watermarking, but they always remain insufficient.

2.1. Definition

2.1.1. Watermarking

Consists in inserting in an invisible and indelible way an information (mark) in an image then to try to recover this information after transfer of the image [23].

2.1.2. Steganography

Steganography is defined as the art of hiding information in a medium. There are two approaches to steganography: [14]:

- the first approach consists in hiding the protected information inside another one. This is called information hiding or data hiding. The principle of this approach is similar to that of cryptography: information is inserted or extracted from the medium by means of codes generated by keys. However, unlike cryptography, the protected information is not visible.
- the second approach to steganography, a signature is embedded in a document or image to protect the document or image from being compromised. This approach is known as watermarking in English or digital tattooing in French. Our work focuses on this approach to steganography.

2.2. Presentation of the Different Existing Digital Image Watermarking Methods

In our literature we have identified two families of methods that deal with digital image watermarking [16]. We can quote the additive methods and the virtual methods.

2.2.1. Additive Methods

In [16], the general scheme of the additive method is presented [16, 17] as well as the different methods of watermarking. First, he talked about adding noise to the image according to the following two methods:

- the method of the Patchwork: this first method consists in adding Patch to certain secret place of the image whose detection is based on the knowledge of its secrets.
- the method of the spread of spectrum: one adds a noise broad band to the image. The message thus spread will thus be present on all the frequencies and will be more resistant to the alterations of this band.

In conclusion [2] demonstrated that patchwork methods and spread spectrum methods work on the same principle.

Secondly [2], he talked about the use of transformed domain. Additive watermarking algorithms can work in any transformed domain of the image, provided that the transformation is invertible. Here, noise is added uniformly to the pixel values of the image. In this section we can mention transforms such as the discrete cosine transform (DCT), the discrete wavelet transform (DWT), the Fourrier-Mellin transform, and the complex wavelet transform.

2.2.2. Virtual Methods

The virtual watermark is the one where the mark is not added on the data but the mark imposes constraints on the image values. [16] explains this method in his article. First he talked about the use of JPEG compression, then the use of fractal compression and finally the use of quantizers.

In view of all that has been said in the literature we can say that the virtual method is a technique that is non-invertible. Then the hacker (a malicious person) cannot remove the inserted mark once he intercepts the image. The only thing he can do with it is to destroy the image completely. This technique is robust because of the constraints it imposes. The advantage of this method is the mark that is imposed on the image structure. It is necessary to remember that the key and the mark are of great size [16].

2.3. Different types of Attacks

The attack is defined as being any treatment likely to deteriorate the mark or to cause an ambiguity at the time of its extraction [22, 21]. There are mainly two main families of attacks:

- benevolent attack: regroups the manipulations carried out by a user (the designers) which do not have initially for objective to prevent the detection of the mark. In addition, these manipulations can be combined to create more complex attacks. They create these types of attacks to find flaws in their system in order to provide robust solutions.
- malicious attack: includes operations that aim to remove or prevent the correct extraction of the mark. In general, these types of attacks are aimed at making changes to the original image or swapping the original image.

According to [13] there are in the literature two main classifications detailing the different attacks that an image can undergo. We can quote Hartung et al [10] who explain the first classification in their articles, and the second classification is the one proposed by Voloshynovskiy et al [29, 30] and [26]. The following Figure 1 represents the said classification.

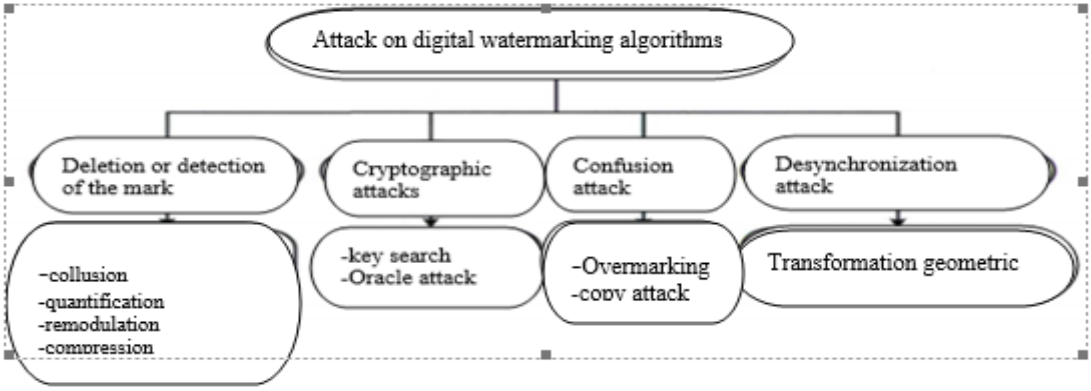

Figure 1. Classification of attacks by Voloshynovskiy et al [29, 30]

2.4. Different Attack Techniques

the literature we read several articles which treat of its various techniques of attack. We can quote ref19, ref20, ref21 in their article devoted to the attacks of the medical imageries, quoted the following attack techniques: the JPEG compression, the blur, the addition of Gaussian noise, the rotation: in this attack the mark is destroyed, the cropping, the pixelization, the accentuation, the histogram, the intensity adjustment and the gamma correction. It is necessary to note also the geometry attacks. For [7] him the validation of a technique can take importance only by testing it against various types of attacks. The attack by filtering: the inserted mark is destroyed. The attack by resizing: The tattooed images are resized to a percentage geometry" Presented on June 14, 2015 by Mr... BELAHRECHE MOHAMED" [19]. In his paper he describes the attack techniques, it should be noted that these techniques are robust, however they are fragile against attacks geometry [19]. To take up the challenge we will base ourselves on the principle of Harris. [16] presents in the table I the various types of attack which can undergo a watermarked image.

Table 1. classification of attacks [16]

Attack on the implementation	**Attack on detection**
Cropping	affine applications
Filtering	Addition of noise
Compression	Jitter attack
Denoising	Switching to analog
Averaging	Stirmark
Impasse	Unsign
	Mosaïque
	Collusion
	Surmarquage
	Copiage
	Natural False Alarms

3. METHODOLOGY

3.1. Watermark Model

In this section we will discuss only the mathematical demonstrations that will lead to a uniform equation. We will not rewrite them, but just give the references.

In Garcia Vincent [28] and Sylvie CHAMBON [4] explain the same principles. In [13], he demonstrates the processes of insertion and extraction using mathematical formulas

Note that the function f computed in (x, y) by Moravec, given a pixel (x, y) of the image and a spatial shift $(\delta x, \delta y)$, and I is image original, it defines its function by

$$f(x, y, \delta x, \delta y) = \sum_{w} (I(\delta x, \delta y) - (x, y, \delta x, \delta y))^2 \quad (1)$$

which is the final function found by Moravec.

Note that Harris and Stephens defined their function as follows: Given an offset $(X, Y, \delta x, \delta y)$ is defined by:

$$f(x, y, \delta x, \delta y) = \sum_{w} (I(\delta x, \delta y) - (x, y, \delta x, \delta y))^2 \quad (2)$$

Seeing that equation (1) is equal to equation (2) we conclude that Harris and Stephen are on the same principle.

Thus the Harris and Moravec methods are well suited to create a robust watermark. The Moravec detector responds too strongly to contours because only the minimum of ɛ is taken into account in each pixel. The Moravec matrix is as follows:

$$\Delta(x, y) = \begin{bmatrix} (G_\sigma * (\frac{\partial_1}{\partial_x})^2)(x, y) & G_\sigma * (\frac{\partial_1}{\partial_x} . \frac{\partial_1}{\partial_y})(x, y) \\ G_\sigma * (\frac{\partial_1}{\partial_x} . \frac{\partial_1}{\partial_y})(x, y) & (G_\sigma * (\frac{\partial_1}{\partial_x})^2)(x, y) \end{bmatrix} \quad (3)$$

With Moravec the eigenvalues (λ_1 ,λ_2) of the matrix A we calculate, while Harris and Stephens proposed to avoid the tedious calculation of the eigenvalues by studying the determinant and the trace of the matrix A. We thought it best to do the tedious computation of the eigenvalues and then compute the determinants to obtain a result without doubt. Because the eigenvalues form a description of the matrix A invariant to rotations and with the Harris *C* function that allows us to detect the corners and contours of the image detected. The function C defines as follows:

$$c(x, y) = \lambda_1 \lambda_2 - k(\lambda_1 + \lambda_2)^2 \quad (4)$$

$$= det(A(x, y)) - k.trace^2(A(x, y)) \quad (5)$$

In conclusion, the combination of these two methods is robust to attacks [13, 21].We found that it is much more interesting to use this technique to filter medical images, given their robustness to geometric type attacks. For equations (1) to (5), Khaled Loukhaoukha has explained all the symbols in his paper.

3.2. Process

In this section we will show the process of inserting a mark in a medical image. The points of interest are constructed in such a way that in order to reconstruct the original image, it is feasible. The Harris detector is a very popular corner detector. In our readings we have found point of interest detectors. In this section we will discuss these detectors. [28] and [23] spoke mainly about these detectors:

- Lindeberg proposed in [18] in 1998 his multi-scale interest point detector named LoG (for Laplacian of the Gaussian); the detected points are thus invariant to scale changes. We speak of blobs detection rather than points detection because the detection shows regions of interest and not points of interest.
- Moravec's detector [28] suffers from many limitations which makes it work in a limited context. For him the detector function has its limits which he explained in his article in section 3.2.3.
- Harris and Stephen identified some of these limitations of Moravec and, by correcting them, proposed in 1988 a detector of corners known under the name of detector of Harris [27, 1, 4].
- following the work of Harris and Stephens [27] of Lindeberg [18], Mikolajczyk and Schmid propose in [18] a multi-scale detector of points of interest. This point of interest named Harris-Laplace, using the advantages of these two methods. Namely the performance of the Harris detector coupled with the multi-scale aspect used by Lindeberg with the LoG detector.

Considering all these corner detectors we found the one of Harris and Stephens more adapted in our context. But to prove the robustness, we decided to keep the combination of the two methods, namely Harris and Moravec. We found that the detector proposed by Mikolajczyk and Schmid does not meet all the requirements of robustness. For the combination with the Lindeberg method which uses blobs rather than points of interest detection are fragile to certain types of attacks such as geometry attacks. On the other hand Moravec uses points of interest so for us it is a perfect combination to reinforce the Harris method. Figure 2 shows the points of interest of a random image that will constitute the signature of the doctor.

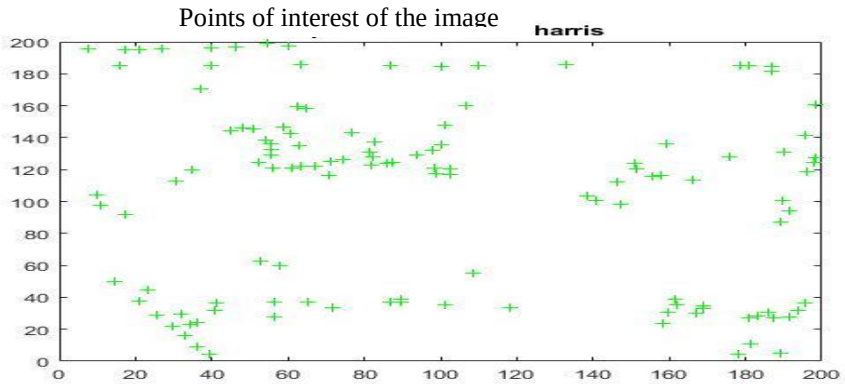

Figure 2: Points of interest of the image

3.3. Context

The general scheme of a digital watermarking system can be described mainly by two fundamental phases: insertion and extraction. However a third stage can be considered: as the transmission. Figure 3 following presents this sequence which is described in [13].

For him the first phase consists in inserting in the original image noted I_o a mark M, and a secret key C_w of the marking to obtain the tattooed image I_w.

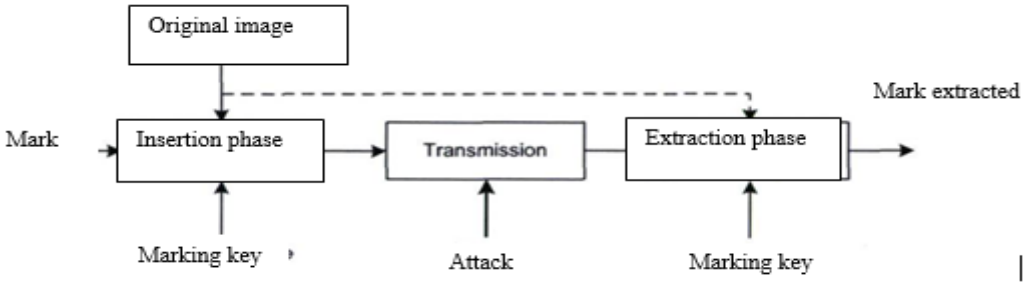

Figure 3: General diagram of insertion, transmission and extraction of the mark [13]

$$M = \{M_1, M_2 \cdot \cdots M_{n1} \cdot\} \in M^{n1} \qquad (6)$$

we obtain the mark to insert W defined by.

$$W = \{W_1, W_2 \cdot \cdots W_{n2} \cdot\} \in W^{n2} \qquad (7)$$

The use of a mark generation function Fm. The generation of the mark is defined mathematically as follows.

$$M^{n1} x C_w \longrightarrow W^{n2} Fm : (M, C_w)\ 7 \longrightarrow W \qquad (8)$$

After having obtained the mark to be inserted we will proceed to the insertion. At this level we have to generate the watermarked image I_w from the mark W and the original image I_o. F_i is the mark insertion function. We obtain the following sequences.

$$S = \{S_1, S_2 \cdot \cdots S_n \cdot\} \in S^n, \qquad (9)$$

$$and,\ Sw = \{Sw1, Sw2 \cdot \cdots Swn \cdot\} \in S^n \qquad (10)$$

$$W = \{W_1, W_2 \cdot \cdots W_{n2} \cdot\} \in W^{n2} \qquad (11)$$

$$With\ c, n_1 > n_2, S_w = F_i(S, W) \qquad (12)$$

During the extraction of the image, when one needs the original image I0 one speaks about informed or not blind watermarking [13]. In the contrary case one speaks about not informed or blind watermark. According to him the informed watermark allows to know if the image underwent geometrical transformations or not. This is where Harris brings an advantage to digital watermarking.

3.4. Expected results

In this section we will apply our method on a medical image to get the watermark containing the mark, and who will be able to send on the network in full safety.

3.4.1. Advantage of points of Interest

- More reliable sources of information than contours because more constraints on the intensity function.
- Robust to occultations (either completely occulted or visible).
- Easier to extract than contours.
- Present in a large majority of images (≠ contours!).
- Points of interest not discontinuous in one direction like contours
- Robust to all types of attack

3.4.2. Performance Criterion

Figure 4 represents schematically the problem of the digital watermark [25]. This problematic is well explained in [25].

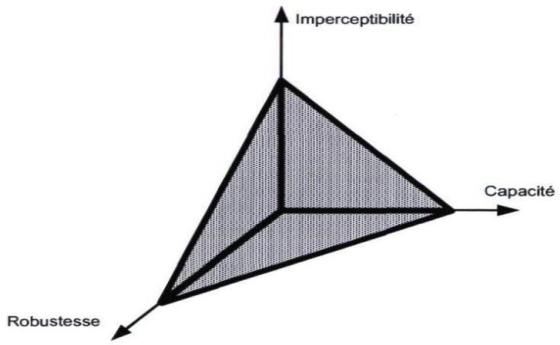

Figure 4: The problem of digital tattooing [25]

In [13] and [20, 25, 6], they explain clearly these three criteria of the robustness of a digital watermark. For them it is thus necessary to find the best possible compromise between these three parameters according to the envisaged application.

- Capacity: represents the quantity of information which one wants to insert in an image. In general, a few bits are enough for copyright protection with an identifier, but not for inserting a company logo.
- Imperceptibility: This constraint requires that the said distortions are as low as possible so that visually the watermarked image remains faithful to the original image. The quality of the watermarked image compared to the original image can be evaluated using mathematical tools such as the peak signal to noise ratio (PSNR), structural similarity (SSIM), etc. The imperceptibility criterion is a property related only to the invisible digital watermarking.
- Robustness: the ability to recover the inserted mark even if the watermarked image has been manipulated by attacks.

3.5. Evaluation Criterion

The complete evaluation of a watermarking scheme requires to define precisely, for each characteristic (imperceptibility, reliability, capacity, speed), a desired level of assurance [Automatic evaluation of watermarking schemes]. For [25] no schedule of conditions really gives fixed values to measure the robustness of a watermarking algorithm. For him the visual quality is an effective means to validate a digital watermarking algorithm. As regards the measures of quality of the image one refers to measures which are:

- Either subjective: here the watermarked image and the original image are put in test [8].
- Either objective: [8] the objective measurements are based on the comparison pixel by pixel between the original image and the marked image. Among these measures we find the Relative Entropy, the Mean Square Error, the Mean Absolute Error, the Signal to Noise Ratio (SNR) and Weighted SNR.

In order to evaluate the reliability of a watermarking technique we will use two crucial metrics which are: the detection efficiency and the PSNR which determines the degree of imperceptibility of the mark.

- The PSNR: Peak Signal Noise Ratio: The PSNR is a function of the MSE. It makes it possible to determine the variation that the image underwent. In other words the degradation of the original image in db caused by the insertion of the mark, by the compression of the image or by another attack. The PSNR is defined as follows.

$$PSNR = 10\log10(255^2/MSE) \qquad (13)$$

- The MSE represents the mean square error between the studied image and the original one in order to evaluate the influence of the variation on the image. It is defined as follows:

$$MSE = \frac{\sum_i \sum_j (I_{ij} - I^*_{ij}))}{mn} \qquad (14)$$

I and I^* are respectively the original image and the watermarked image of size m×n with I_{ij} and I_{ij^*} their components. He goes even further to determine the efficiency of the detection E

- Detection efficiency

$$E = \frac{N_{ad}}{N_d} * 100 \qquad (15)$$

ou N_{ad} the number of affected blocks detected.

N_d the number of blocks.

3.6. Simulation

In this section we will use the Harris detector to insert a mark in a medical image. First we have to choose a random image (which can be any other medical image or not) and then use the Harris detector to extract only the points of interest from this image. At the end we will have two images, that is to say the one with the points of interest only and the rest of the image.

The insertion of the data in the image will follow the following steps:

1. Take a random image (which can be a medical image or not).
2. Take the original patient image (the patient data you wish to transmit).
3. Use the Harris function (Harris detector) to extract the points of interest from the random image.

4. Finally, use the Harris function to add the points of interest to the original image of the patient.

We then obtain a watermarked image that is resistant to the various attacks. Mathematically [13] describes all the processes of insertion of the mark with mathematical formulas. As for the Figure 5 shows us the points of interest obtained from any image.

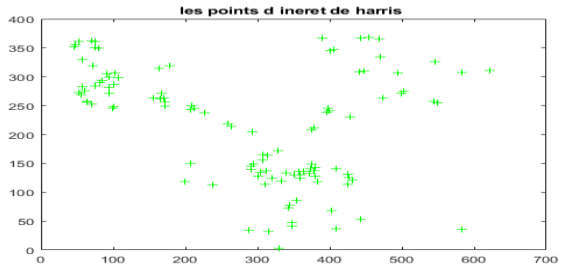

Figure 5: Points of interest extracted from the original image

Once we have the points of interest (in this case the mark to be inserted) we now proceed to add the mark to the original image. It should be noted that we are in the case of the invisible watermark so the mark to be inserted in the original image must not lose the imperceptibility of the image. The following figure 6 shows the watermarked image.

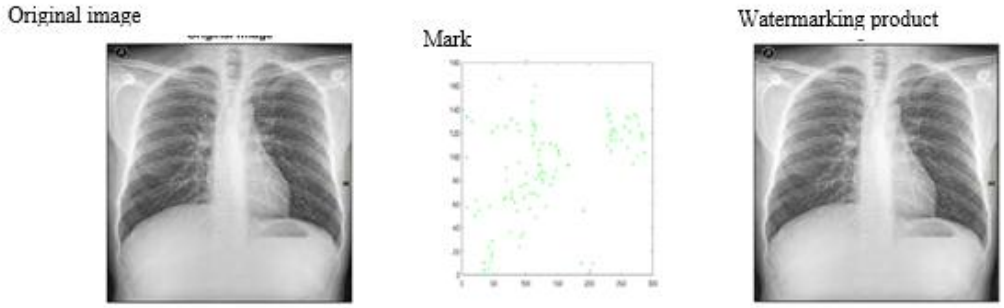

Figure 6: Product watermark

On the Figure 7 is presented the watermarked image that will be sent by the doctor.

Figure 7: Watermarked medical image to be sent

In this section we will proceed to the extraction of the patient's data as well as the signature (points of interest of the random image) of the hospital or the doctor. The extraction process will consist in extracting the mark that the sender has inserted in the original image. [25] There are two modes of extraction of the mark according to the various techniques of the watermark, the original image can be necessary or not during the detection of the mark.

- blind watermark: the extraction or detection of the mark is done with the image to be analyzed and the mark. The hidden information must be detected directly from the image to be analyzed without using the original image.
- non-blind watermark: requires the original image to extract the mark is called non-blind watermark. It is more robust than the blind watermark but is less used because it requires the original image.

The Harris principle we use requires the original image to extract the mark from the image. So the non-blind watermark will be the one we will use to extract the mark from our image. The following Figure 8 show the extraction of the mark previously inserted in the original image.

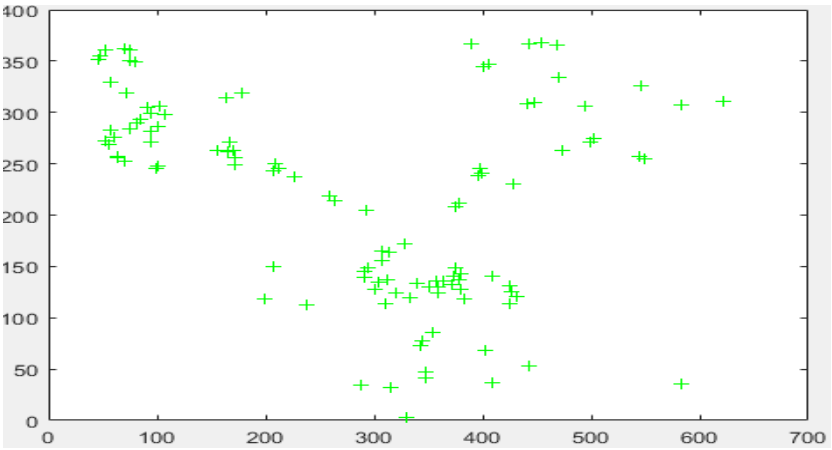

Figure 8: Mark extracted from the watermark

It should be noted that there is no difference between the watermarked image and the original image. One of our first goals was to tattoo the image without the difference between the original image and the one containing the mark.

3.7. Interpretation

Given the multiple applications considered as well as the criteria that come into play, it is difficult to evaluate a watermark algorithm, however it is possible to identify some essential elements for the evaluation of watermark such as the digital watermarking algorithm in terms of imperceptibility and the robustness of the technique against the various attacks [8].

Our contribution is referred to [9] In this part we will make a comparison of the images in term of imperceptibility between the proposed algorithm. The inserted Watermark must be completely invisible by the Human Visual System (HVS) [12]. To prove the imperceptibility of the image we will make a comparison of the images: watermarked image and the original image.

It should be noted that we will be interested in Mean Square Error: MSE and Peak Signal to Noise Ratio: PSNR, but it should be noted that other measures are necessary such as Mean Absolute Error: MAE, Signal to Noise Ratio: SNR, Enhancement Measurement Error: EMA.

The following Table 2 shows a comparison between the watermarked image and the original image. It should be noted that we had used an original image and then added a mark and we get the watermarked image, since our method respects the principle of imperceptibility then the SVH will not be able to make the difference between the two images. So, we will calculate the PSNR and MSE to show their resemblance and their difference too.

In the case where the image has not been watermarked i.e., the images are equal (original or watermarked). The following Table 2 shows their resemblance.

In the case where the image has not been watermarked i.e. the images are equal (original or watermarked). As example in Table 2 firstly and secondary the both images is equal.

To know if the two images are equal, we must compare their MSE and PSNR. It should be noted that in this part if the MSE = 0 and the PSNR = 99 or 100 we conclude that the images are equal. We used three types of images namely X-ray, CT and ultrasound and then we compared each image with its watermark to calculate their PSNR and MSE. In the Table 2 we calculated the PSNR and MSE of the watermarked image and the original image this shows the veracity of the watermark.

The table 2 summarizes the difference between the MSE and the PSNR of the watermarked images and their originals. These coefficients of MSE and PSNR allow to judge the existence and the accuracy of the tattoo. This table allows us to justify the imperceptibility of the medical watermark.

Table 2: Image quality and relationship between PSNR and MSE

Original Image	**Watermarked Image**	**PSNR**	**MSE**
Watermarked Image	Watermarked Image	99	0.0
Original Image	Original Image	99	0.0
Images Scanner	Watermarked	30.2755	61.0282
Image radiography	Watermarked	10.014	40.0552
Image cerography	Watermarked	40.1455	80.05748

4. CONCLUSION AND PERSPECTIVES

In our paper we have based on the Harris method in the field of digital image watermarking, especially in the field of medical imaging, with the objective to evaluate the robustness of the method. The application of this technique gives better results on the quality of the watermarked image and the robustness of the watermark. It should be noted that the two fundamental properties which are the imperceptibility and the indelibility were respected. The contribution to this topic was to prove the robustness of the Harris method to design a watermark resistant to different types of attacks such as rotation and geometry transforms. We also made a comparative analysis between the original image and the watermarked image. In this part we used PSNR and MSE for each image to verify the fundamental property which is the imperceptibility of the watermarked image. We are convinced that the Harris method based on the Moravec principle is robust.

As perspectives it should be noted that the attack of the watermarked image on the network could be the subject of study. The Harris principle is considered good for watermarking with projections based on hyperbolic geometry combined with the point-square disk. The next contribution will be

to take the watermark obtained with the Harris principle to make a hypercatadioptric projection in order to obtain a robust digital image watermark resistant to all kinds of attacks.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] M Karoud S Najah A Aarab and M Mrabti."Tatouage d'Images: une nouvelle approche basee sur les points d'intérêts" . In: (March 25-29, 2007).
[2] Patrick Bas. "Methodes de tatouage d'images´ fondees sur le contenu". PhD thesis. Editeur´ inconnu, 2000.
[3] Ryma Dr BOUSSAYOUD et al. "Cryptage, Chiffrement et Tatouage des donnees´ numeriques". In: (Feb. 1, 2010).´
[4] Sylvie CHAMBON. "Projet MARIO Detection de points d'interet". In: (13 janvier 2007 – 2/11 Page 4).ˆ
[5] Franck Davoine and Stephane Pateux.´ Tatouage de documents audiovisuels numeriques´ . Hermes` Science Publications, 2004. 277 pp. URL: https: //hal.archives-ouvertes.fr/hal-00093925 (2004).
[6] Imen FOURATI and Med Bouhlel. "Elaboration d'une nouvelle approche de tatouage fragile des images medicales". In: (Nov. 7, 2020).´
[7] Imen Fourati and Mohamed Salim Bouhlel. "Elaboration d'une nouvelle approche de tatouage fragile des images medicales". In: Sciences Electroniques, Technologies de l'Information et des Telecommunications SETIT 2005. 2005.
[8] Mohamed Ali Hajjaji et al. "A new system for watermarking based on the turbo-codes and wavelet 5/3". In: 13th International conference on Sciences and Techniques of Automatic control & computer engineering. 2012.
[9] Mohamed Ali Hajjaji et al. "Tatouage des images medicales en vue d'int´ egrit´ e et de confiden-´ tialite des données". In:´ CINQUIEME WORKSHOP AMINA 2010" Applications Medicales de´ l'Informatique: Nouvelles Approches". 2010.
[10] Frank H Hartung, Jonathan K Su, and Bernd Girod. "Spread spectrum watermarking: Malicious attacks and counterattacks". In: Security and Watermarking of Multimedia Contents. Vol. 3657. International Society for Optics and Photonics. 1999, pp. 147–158.
[11] Mohamed Karasad. "Tatouage des images medicales partagées". PhD thesis. Ecole nationale superieure Mines-Télécom Atlantique,´ June 25, 2018. URL: https://tel.archives-ouvertes. fr/tel-02867836 (visited on 10/15/2020).
[12] Ammar Lahlouhi et al. "Tatouage numerique des images couleurs RGB". In: (03 Apr 2017 12:39), p. 128.
[13] Khaled Loukhaoukha. "Tatouage numerique des images dans le domaine des ondelettes base´ sur la decomposition en valeurs singulières et l'optimisation multi-objective". In: (2010). Accepted: 2018-04-17T21:25:37Z. URL: https : / / corpus.ulaval.ca/jspui/handle/20.500.11794/ 22208 (visited on 10/07/2020).
[14] Telesphore Tiendrebeogo · Maria Moloney · Tegawende F. Bissyand´ e ·Damien Magoni. "Ro-´ bust Formal Watermarking Model Based on the Hyperbolic Geometry for Image Security". In: (2019). Accepted: 2019-04-17T21:25:37Z. URL: https://corpus.ulaval.ca/jspui/handle/20.500. 11794/22208 (visited on 10/07/2020).
[15] Unmesh Mandal, Kumar Samir, and Samir Bandyopadhyay. "Visible and Invisible Watermarking using Discrete Wavelet Transform". In: (June 1, 2015).
[16] Anne Manoury. "Tatouage d'images numeriques´ par paquets d'ondelettes". PhD thesis. Ecole Centrale de Nantes (ECN); Universite de Nantes,´ 2001.
[17] Amit Mehto and Neelesh Mehra. "Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT". In: Procedia Computer Science 78 (2016), pp. 88–94. ISSN: 18770509. DOI: 10 . 1016 / j . procs . 2016 . 02 . 015. URL: https : / / linkinghub. elsevier. com / retrieve / pii / S187705091600017X (visited on 10/15/2020).

[18] Krystian Mikolajczyk and Cordelia Schmid. “Indexation a l’aide de points d’int` er´ ets invariantsˆ a l’` echelle”. In:´ Journees ORASIS GDR-PRC´ Communication Homme-Machine. 2001, pp. 77– 86.
[19] Mr BELAHRECHE MOHAMED. “Memoire de master domaine: Sciences Techniques filiere electronique”. In: (le 14 juin 2015 par).
[20] Imen Nouioua. “Developpement´ et implementation´ d’algorithmes de tatouage numerique des donn´ ees multim´ edia”. Accepted:´ 2019-07-10T07:46:08Z. Thesis. July 10, 2019. URL: http : / / dspace . univ - setif . dz : 8888/jspui/handle/123456789/3440 (visited on 11/07/2020).
[21] Fabien AP Petitcolas, Ross J Anderson, and Markus G Kuhn. “Attacks on copyright marking”. In: Proc. 2nd Workshop on Information Hiding, Portland/Oregon, April 1998. 1999, pp. 219–239.
[22] Fabien AP Petitcolas, Ross J Anderson, and Markus G Kuhn. “Attacks on copyright marking systems”. In: International workshop on information hiding. Springer. 1998, pp. 218–238.
[23] William Puech, Michel Dumas, and Jean-Claude Borie. “Tatouage d’images cryptees pour l’aide´ au tel´ ediagnostic”. In: (), p. 4.´
[24] Christian Rey and Jean-Luc DUGELAY. “Un panorama des methodes de tatouage permettant´ d’assurer un service d’integrit´ e pour les im-´ ages”. In: TS Traitement du Signal 18.4 (2001), pp. 283–295.
[25] Rabia Riad. “Tatouage robuste d’images imprimees”. PhD thesis. Universit´ e d’Orl´ eans; Uni-´ versite Ibn Zohr (Agadir), 2015.´
[26] Shrikhande Rohini and Vinayak Bairagi. “Lossless medical image security”. In: International Journal of Applied Engineering Research, Dindigul 1.3 (2010), pp. 536–541.
[27] Nizar Sallem and Michel Devy. “Modelisation´ d’Objets 3D en vue de leur reconnaissance et leur manipulation par un robot personnel”. In: ORASIS’09-Congres des jeunes chercheurs en` vision par ordinateur. 2009.
[28] Garcia Vincent. “Suivi d’objets d’inter´ et dansˆ une sequence d’images: des points saillants aux´ mesures statistiques”. PhD thesis. Universite´ Nice Sophia Antipolis, 2008.
[29] Sviatolsav Voloshynovskiy et al. “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks”. In: IEEE communications Magazine 39.8 (2001), pp. 118– 126.
[30] Min Wu and Bede Liu. “Attacks on digital watermarks”. In: Conference Record of the ThirtyThird Asilomar Conference on Signals, Systems, and Computers (Cat. No. CH37020). Vol. 2. IEEE. 1999, pp. 1508–1512.

AUTHOR

Maliki BADOLO, master degree in information systems and decision support system in nazi BONI university Burkina Faso. My interest research topic is image watermarking for decision support and multimedia system.

Telesphore Tiendrebeogo PhD and overlay network and assistant professor at Nazi Boni University. I have a master's degree in multimedia and real time system. My current research is on big data and image watermarking