MULTIPLE IMAGE WATERMARKING BASED ON SVD : IMPROVING CAPACITY AND IMPERCEPTIBILITY

Henri Bruno Razafindradina[1] and Paul Auguste Randriamitantsoa[2]

[1]Department of Electrical Engineering, Higher Institute of Technology, Diego-Suarez, Madagascar
[2]Department of Telecommunications, Higher Polytechnic School, Antananarivo, Madagascar

ABSTRACT

Digital watermarking consists of inserting a mark (text, image, sound or video) in a medium. The goal is to be able to identify the author or owner of a digital document by the inserted mark. Watermarking algorithms must find a compromise between capacity and imperceptibility. Capacity represents the amount of data inserted and the imperceptibility makes the mark invisible. Our research is related to images watermarking based on singular value decomposition. There are two main approaches to improving capacity and imperceptibility : dual technique and multiple technique. Most algorithms based on these two approaches have low capacity : the watermarks are generally smaller than the host image. Agarwal & al worked on inserting an image into another image of the same size, imperceptibly. Their method adds the mark in the V matrix of the image after its singular value decomposition. A λ parameter was chosen to specify the power of insertion. Our contribution is to add two images by simultaneously improving capacity and imperceptibility. This new method consists on adding the mark in the 2 matrices U and V after singular value decomposition. The insertion of the first mark is an addition as in Agarwal's method while that of the second mark is a subtraction to make the watermark less imperceptible. The result shows that our method is robust against different attacks such as compression, noise addition, median filtering and rotation. It is also imperceptible because not only we obtain a PSNR of 27 dB, but the histogram obtained is closer to that of the original image than that of Agarwal. A test on a database of 180 images shows that the marks are still detected. However, despite these advantages, the first mark is less visible and of poor quality compared to the second after their extraction. One solution to this is to increase the value of the parameter λ for the insertion of the first mark.

KEYWORDS

Watermarking, Singular Value, Capacity, Imperceptibility.

1. INTRODUCTION

The Internet, the power of computers, standards organizations and the development of multimedia processing software have made it easy to popularize and spread multimedia documents (text, images, sounds and videos, etc.). It has become easy even for simple users to copy, hack such documents without the authorization of their authors. Watermarking is a technique for inserting the author's mark (brand) into his work so that he can extract it at the right time in order to protect it from unauthorized uses. Image watermarking based on singular value decomposition [1] is one of the most used techniques currently for inserting mark of the same size as the original image. New techniques have emerged that involve inserting two marks to identify the owner and detect potential intentional attacks. Mohanty [2] presented a watermarking algorithm called dual watermarking technique that is a combination of visible and an invisible watermark. Following this idea, Khare [3] presented a dual technique that embeds watermarks on

DOI:10.5121/ijcis.2022.12401

HL and LH subbands after DWT transformation. Others researchers discussed about new techniques allowing multiple watermark. Contrary to dual watermarking, multiple watermarking inserts several invisible marks into a host image. Ananth [4] presented a robust multiple successive and segmented watermarking technique based on Wavelet Domain for host image of size 512×512 and 2 watermarks of size 48×48. Noruhida and Surekha [5][6][7] developed another multiple watermarking technique that embeds 2 small binary watermarks. Mohananthini [8][9] inserted two gray scale watermark images (32×32 size) into the original color image (512×512 size) using the Daubechies Wavelet Transform and studied its applications in medecine. Bastani and Sharkas technique [10][11] allows to insert two marks whose dimension is a quarter of that of the host image. Inamdar [12] have proposed a complex dual watermarking scheme with multiple biometric watermarks in which it embeds firstly speech and face biometric traits of owner and lastly offline signature is overlaid translucently on image. Most of those techniques are limited in capacity because the size of the watermark is one quarter or half that of the host image.

Our approach allows to add 2 marks of the same size as the host image, based on the Agarwal's insertion process [13]. The first mark is the owner's logo and the second is that of the organization guaranteeing intellectual property. In this paper, the fundamental principles of watermarking based on singular value decomposition are first recalled, our dual approach is then detailed and the obtained experimental results are discussed.

2. SINGULAR VALUE DECOMPOSITION

Singular value decomposition is a technique of linear algebra having applications in various fields : matrix inversion, low-dimensional representation of high dimensional data, watermarking [1][14], data compression [15][16][17], data encryption [18][19][20], etc. For any m×n matrix I, it is possible to find a decomposition of the form $I = U\ S\ V^T$, (1) where U and V are orthogonal matrices of order m×m and n×n respectively. The diagonal matrix S of order m×n has elements s_{ii},(i = 1, 2, …, r), defined positive and called singular values. r is called the rank of the matrix I.

2.1. Algorithm for Inserting a Mark into a Grayscale Image

This section presents Agarwal's algorithm [13] for inserting a grayscale image into another grayscale image of the same size using SVD. Let the matrix I represent the host image to be marked. Let W representing the matrix of the image to be inserted.

Step 1, decomposition of I and W.

For the host image

$I = U_I\ S_I\ V_I^T = A_I\ V_I^T$ (2)

For the mark

$W = U_W\ S_W\ V_W^T = A_W\ V_W^T$ (3)

where $A_{I/W} = U_{I/W}\ D_{I/W}$ is also called the principal component.

Step 2, adding the mark in the V_I matrix

Now, we can add the V_W weighted eigenvector of the mark to that of the original image, $V = V_I + \lambda V_W$ (4) where λ is the scaling factor. Typically, $0 \leq \lambda \leq 1$, so that the mark is as imperceptible as possible. Note that, in SVD, $V_W V_W^T = Id$, where Id is the identity matrix. A similar relationship also holds for V_I.

Step 3, calculation of the marked image

We obtain the marked image with $I_W = A_I V^T$ (5)

2.2. Extraction Algorithm

Given the watermarked image I_W, we can extract, the mark, if we have access to the A_I, A_W, V_I matrices and λ parameter. That is, anyone wishing to extract the mark must have access to the original image as well as the marked image.

The extraction algorithm is an inversion of the insertion algorithm given in the previous paragraph. Multiplying both sides of equation (5) by A_I^{-1} and subtracting V^T from equation (4) returns an expression for V_W^T with $V_W^T = (A_I^{-1} I_W - V_I^T)/\lambda$ (6)

Finally, using equation (3), the mark can be reconstructed as $W_r = A_W V_W^T$ (7)

3. Our Method

Our method proposes to insert two marks in the host image. It works only on raster image. One is the author's logo, the other is that of the third-party organization that authenticates the mark. The idea is to find a compromise between the capacity representing the amount of data inserted and the imperceptibility making the mark invisible to the naked eye.

3.1. Algorithm for Inserting Two Marks

Let I be the host image, W_1 the author’s mark and W_2 the organization’s logo

Step 1, decomposition of I, W_1 and W_2.

$I = U_I S_I V_I^T$ (8)
$W_1 = U_{W1} S_{W1} V_{W1}^T$ (9)
$W_2 = U_{W2} S_{W2} V_{W2}^T$ (10)

Step 2, inserting the two marks

The eigenvector V_{W1} of the author's mark is inserted to that of the original image, $V_1 = V_I + \lambda V_{W1}$

(11).The organisation's logo eigenvector U_{W2} is inserted into that of the original image, $U_2 = U_I - \lambda U_{W2}$

(12). Subtraction is chosen on the assumption that it would counterbalance the first insertion made with addition. This second insertion uses the same scaling factor λ.

Step 3, calculation of the marked image

A watermarked image is obtained with $I_W = U_2\ S_I\ V_1^T$ (13). That means we can reconstruct the image with the 2 unitary modified matrices (U_2 and V_1) and the singular values matrix S_I. After their modification, $U_2\ U_2^T \sim Id$ and $V_1\ V_1^T \sim Id$ as described in the section 2.1 step 2.

3.2. Algorithm for Extracting the Two Marks

By applying the algorithm of paragraph 2.2, we obtain the expression for V_{W1}^T and that of U_{W2} :
with $V_{W1r}^T = [(U_2\ S_I)^{-1}\ I_W - V_I^T]/\lambda$ (14) et $U_{W2r} = [I_W\ (S_I\ V_1^T)^{-1} + U_I]/\lambda$ (15)
Then the mark can be reconstructed as :
$W_{r1} = U_{W1}\ S_{W1}\ V_{W1r}^T$ (16)
$W_{r2} = U_{W2r}\ S_{W2}\ V_{W2}^T$ (17)

4. RESULTS

We tested the new method with 512×512 images. We have chosen to keep the value of $\lambda = 0.2$ proposed in Agarwal's method [13] because this value allows an acceptable imperceptibility with a PSNR = 25 dB. The following figure shows that the imperceptibility decreases with λ. Indeed, from $\lambda = 0.3$, the PSNR value is less than 24 dB.

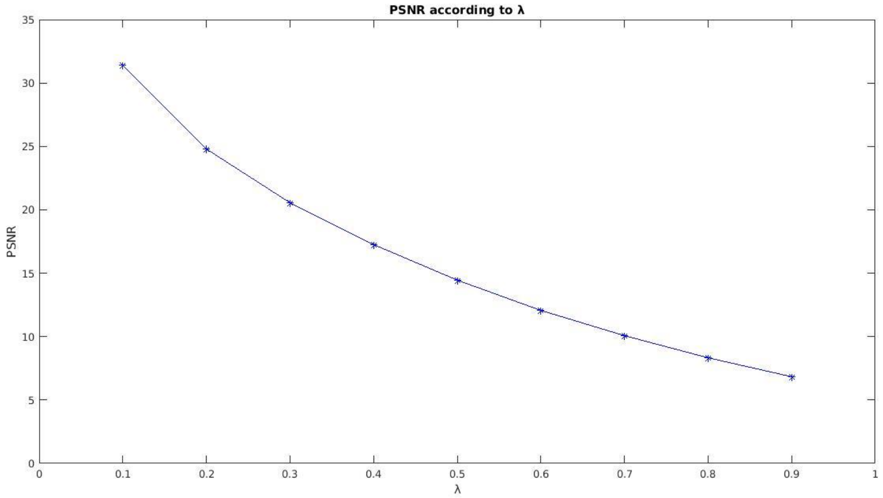
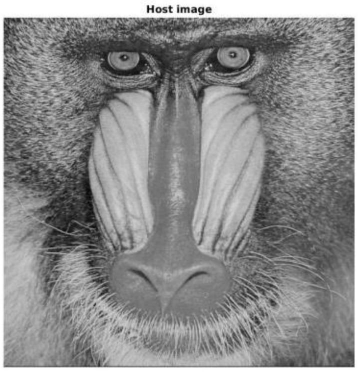
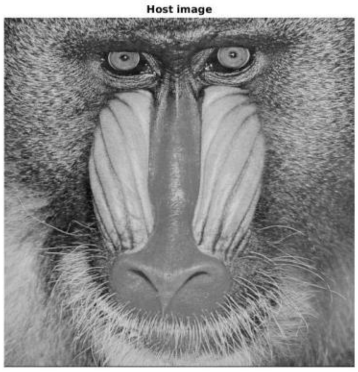


Figure 1. PSNR variation according to λ

The following table summarizes the test images we used for insertion.

Table 1. Test images (host and marks)

Agarwal's method	Our method
	
	
	

We have inserted respectively a mark for the Agarwal method and two marks for our method.

4.1. Imperceptibility

The following figures show the watermarked images. We respectively use the PSNR to assess the imperceptibility of the mark and the histogram to measure the degradation.

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{\mathrm{Max}[I(i,j)]^2}{\mathrm{RMSE}}\right) \quad (18)$$

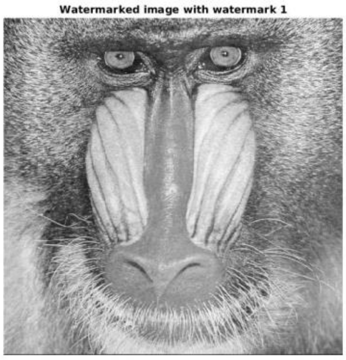
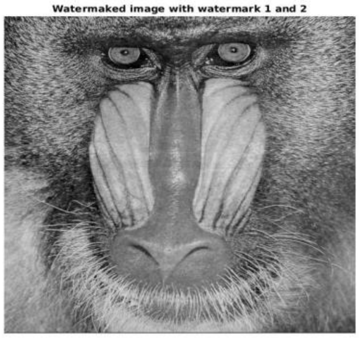
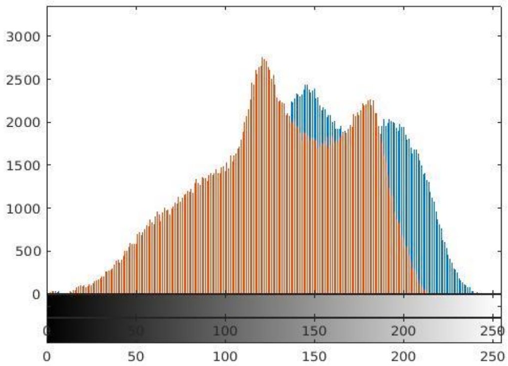
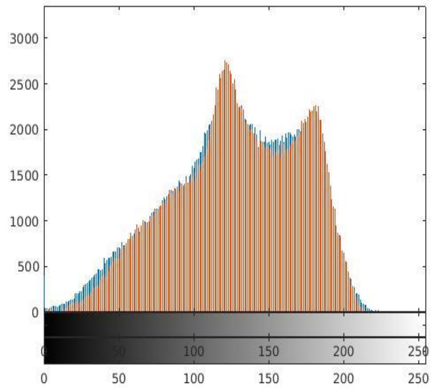
RMSE is the root mean square error :

$$\mathrm{RMSE} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I_W(i,j)]^2 \quad (19)$$

The histogram represents the probability density of light intensities. It is a vector of dimension 256. Each element of the vector h(i) represents the number of pixels of the image having the level of gray i.

PSNR tool is used to measure image quality after mark insertion. The watermarked image with our technique is closer to the original image (PSNR = 27 dB) than the one watermarked with the Agarwal method (PSNR = 21 dB). The histograms obtained also confirm this as they are almost identical while the Agarwal method gives more contrasting images; indeed, the histogram of the watermarked image (blue curve) is shifted by 25 points compared to that of the host image (red curve).

Table 2. Comparison of obtained watermarked images, PSNRs and histograms

Agarwal's method	Our method
	
PSNR = 21 dB	PSNR = 27 dB
	
Histogram of the original image (in red) and that of the watermarked image (in blue) with the Agarwal method	Histogram of the original image (in red) and that of the watermarked image (in blue) with our method

The PSNR of 27 dB only indicates the quality of the watermarked image; the histogram specifies the level of illumination of the image after the insertion of the 2 marks.

4.2. Robustness

The robustness of the method is evaluated by extracting the marks after intentionally modifying the watermarked images (in the hope of eliminating the marks). Two scenarios are considered : the first one is that of a case without attack (the watermarked image has not been modified) and the second one considers the possible attacks already known in the literature.

4.2.1. Nominal Case

The following table summarizes the extracted marks in a normal situation (the image has not been attacked). The 2 marks are well identified after the extraction procedure.

Table 3. Extracted mark

Agarwal's method	Our method
	
	

4.2.2. Attacked Image

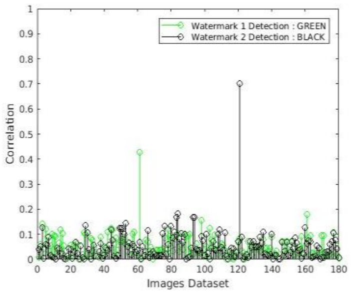
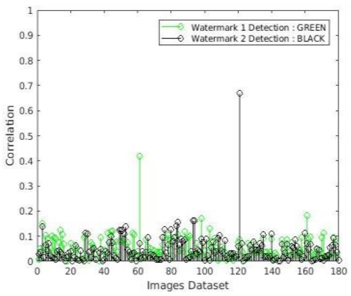
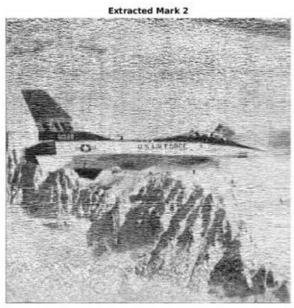
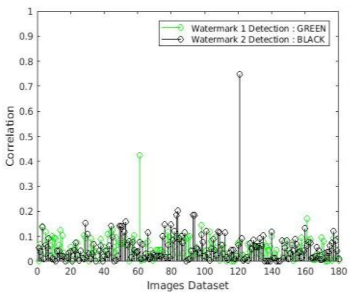
The following table gives the results obtained for different types of attacks: compression, noise, filtering, rotation, etc. The detection of the 2 marks is performed in a database of 180 images. Like other watermarking methods and Agarwal's method precisely [13], ours resists to several types of attacks such as JPEG compression, median filtering, noise addition (Gaussian and pepper), rotation.

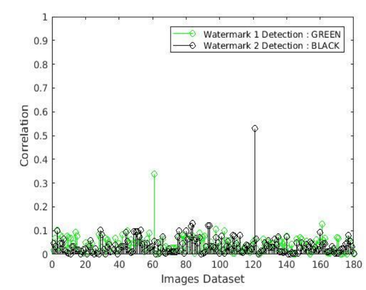
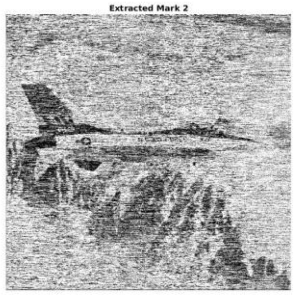
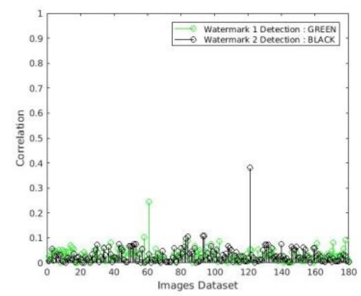
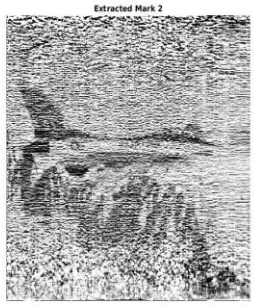
The robustness of the method is evaluated by the correlation between the original mark W and the extracted mark Wr by calculating :

$$\mathrm{corr}(W,W_r) = \frac{\sum_{x=1}^{n}\sum_{y=1}^{n}[W(x,y)-\bar{W}][W_r(x,y)-\bar{W_r}]}{\sqrt{\left(\sum_{x=1}^{n}\sum_{y=1}^{n}[W(x,y)-\bar{W}]^2\right)\left(\sum_{x=1}^{n}\sum_{y=1}^{n}[W_r(x,y)-\bar{W_r}]^2\right)}} \quad (20)$$

The first column shows the correlation coefficients obtained (in green for the detection of mark 1 and in black for mark 2). The remaining 2 columns give the preview of the extracted images. They can be identified with the naked eye despite the attacks on the watermarked image, but the most relevant indicator remains the correlation making it possible to detect the presence of the 2 marks in each image.

Table 4. Extracted marks for different types of attack

Detections	Extracted Mark 1	Extracted Mark 2
Attack : JPEG Compression (Quality Factor 10)		
		
Attack : Median Filter		
		
Attack : Salt & Pepper Noise - Density = 0.02		
		
Attack : Gaussian Noise - Average = 0 and Variance = 0.02		

		
Attack : Rotation 0.5°		
		

We can see that the 2 marks are always detected (frames number 60 and 120) in each attack scenario.

5. Discussion

The objective of the present method is to increase the capacity of the watermark by inserting 2 images of the same size as the host image. The method defies the law that increasing capacity would decrease imperceptibility. Indeed, it even improves imperceptibility because the watermarked image is very close to the host image.

The first mark is, in all cases of detection, darker than the first. This is due to the change of coefficients of the U matrix after the extraction of the second mark.

The method is very sensitive to attack by rotation because an angle greater than 0.5° eliminates the 2 marks

On the other hand, it is very resistant to JPEG compression. A Strong compression with a quality factor of 10 still allows to find easily the 2 marks.

The technique is tested with a database of 180 images. The detection allows to find for each attack the 2 inserted marks. The 2 peaks that are always identifiable confirm the presence of the 2 marks in the watermarked image. The corresponding correlation coefficients are weak for Gaussian noise and rotation attacks, but the 2 peaks are still identifiable; which guarantees the presence of the marks

.

Moreover, despite the poor quality of the first mark (green peak less perceptible than black one), it is still identifiable with the naked eye. To avoid this, we can increase the insertion weight λ of the first mark, but this operation would decrease the imperceptibility characteristic.

The advantage of our method is that we can add 2 marks in a host image: the first one will be the mark of the owner and the second one will be that of the organization that guarantee the copyright. We can also insert the logos of the 2 owners if this is the case.

6. CONCLUSION

Image watermarking is a technique for hiding a watermark (owner's logo) in another copyrighted image. In general, the insertion must meet at least 2 criteria: imperceptibility and robustness. But before building a watermarking algorithm, a compromise must be sought between the following 4 criteria: imperceptibility, insertion ratio, robustness and security. For example, increasing the capacity would affect the imperceptibility or the bit error rate [21]. Our method contributes to the improvement of the first 3 criteria by adding respectively 2 marks (instead of only one) in the 2 unit matrices U and V obtained after the singular value decomposition of the image. The results show that imperceptibility and robustness are improved while keeping the same level of security. The weakness of the method is the poor quality of the first mark which can be solved by increasing its insertion weight λ. Our method introduces the notion of inserting multiple brands within a medium. This gives the possibility for several authors or organizations to claim or prove together ownership of a work. It also guarantees a high level of authentication by being several entities to prove ownership like multiple encryption [22][23][24]. The histogram-based evaluation of the watermarked image can also be improved using Yalman's or Abhishek's method [25][26]

ACKNOWLEDGEMENTS

The authors would like to thank IST-D (Higher Institute of Technology – Diego/Suarez) for its Sponsor and Financial Support.

REFERENCES

[1] Sadek, Rowayda A., (2012) "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 3, No. 7.
[2] Mohanty, Saraju P. & Al, (1999) "A Dual Watermarking Technique for Images", *ACM Multimedia*, Orlando, Florida, pp49–51
[3] Priyank Khare and Vinay Kumar Srivastava, (2021) "A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT", *J. Intell. Syst*, pp297–311
[4] C. Ananth C, Karthikeyan M., Mohananthini N, (2018) "DWT-SVD based Multiple Watermarking Techniques", *International Journal of Engineering Science Invention (IJESI)*, pp01-05
[5] Noruhida Alias, Ferda Ernawan, (2019) "Multiple watermarking technique based on RDWT-SVD and human visual characteristics", *Journal of Theoretical and Applied Information Technology*, Vol. 97. No. 14, pp3980-3989
[6] Noruhida Alias, Ferda Ernawan, (2020) "Multiple watermarking technique using optimal threshold", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 18, No. 1, pp368-376
[7] B. Surekha, G. N. Swamy, K. Srinivasa Rao, (2010) "Multiple Watermarking Technique for Images based on Visual Cryptography", *International Journal of Computer Applications*, Vol.1, No.11
[8] Natarajan Mohananthini and Govindarajan Yamuna, (2013) "Color image multiple watermarking scheme based on discrete wavelet transform", *Proceedings of International Conference "ICSEM'13"*, pp783-787
[9] Natarajan Mohananthini and Govindarajan Yamuna, (2015) "A Study of DWT-SVD Based Multiple Watermarking Scheme for Medical Images", *International Journal of Network Security*, Vol.17, No.5, pp558-568
[10] Bastani, Azadeh & Ahouz, Fatemeh, (2020) "High Capacity and Secure Watermarking for Medical Images using Tchebichef Moments", *RADIOENGINEERING*, Vol. 29, No. 4, pp636-643.

[11] Sharkas, Maha & Al, (2007) "A Dual Digital-Image Watermarking Technique", *World Academy of Science, Engineering and Technology*, pp1477-1480.
[12] Inamdar Vandana S. & Rege Priti P., 2014 "Dual watermarking technique with multiple biometric watermarks", *Indian Academy of Sciences*, Vol. 39, Part 1, pp3–26
[13] Agarwal, Rashmi & Santhanam M.S., (2008) "Digital watermarking in the singular vector domain", *International Journal of Image and Graphics*, Vol. 8, No. 3, pp351–368.
[14] Sura Ramzi Sheriff (2010) "Digital Image Watermarking using Singular Value Decomposition", *Raf. Journal of Comp & Math's*, Vol. 7, No. 3, pp187-199
[15] Kahu, Samruddhi & Rahate, Reena, (2013) "Image Compression using Singular Value Decomposition", *International Journal of Advancements in Research & Technology*, Vol. 2, No. 8.
[16] Santhosh B. Shivani Sinha, Varun Hebbar, Sameer Mohammad, (2019) "Data compression using SVD technique and data storage and distribution using AWS", *SSRN Electronic Journal*, Vol. 6, No. 5, pp257-263.
[17] Mounika K., Sri D., Lakshmi N., Alekya K. (2015) "SVD Based Image Compression", *International Journal of Engineering Research and General Science*, Vol. 3, No. 2.
[18] El Abbadi, Nidhal Khdhair & AL-Rammahi, Adil, (2014) "Text Encryption Based on Singular Value Decomposition", *EUROPEAN ACADEMIC RESEARCH*, Vol. 2, No. 4.
[19] El Abbadi, Nidhal Khdhair & AL-Rammahi, Adil, (2014) "Image Encryption Based on Singular Value Decomposition", *Journal of Computer Science*, Vol. 10, No. 10, pp1222-1230
[20] Ting Yu Liu, Kuan Jen Lin, His chun Wu, (2018) "ECG Data Encryption Then Compression Using Singular Value Decomposition", *IEEE Journal of Biomedical and Health Informatics*, Vol. 22, No. 03, pp707-713
[21] Zhang, Fan & Zhang Hongbin, (2004) "Image digital watermarking capacity and reliability analysis in wavelet domain", *Congrès 47th Midwest symposium on circuits and systems*, MWSCAS '04, pp101
[22] Merkle Ralph, Hellman Martin, (1981) "On the Security of Multiple Encryption", *Communicatino of the ACM*, pp465–467
[23] Hoang V., Tessaro Stefano, (2017) "The Multi-user Security of Double Encryption", *International Conference on the Theory and Application of Cryptographic Techniques*, pp01–35
[24] Harbir Kaur, Hirday Pal Singh Gill, Dipti Sarmah, (2018) "Multiphase and Multiple Encryption", *IEEE Punecon*
[25] Yildiray Yalman, (2012) "A histogram based Image Quality Index", *Przeglad Elektrotechniczny*, Vol. 88, No. 07, pp126-129
[26] Abhishek Tripath, Sudipta Mukhopadhyay, Ashis Kumar Dhara, (2011) "Performance Metrics for Image contrast", *International Conference Information Processing*, pp1-4

AUTHORS

Henri Bruno Razafindradina was born in Fianarantsoa, Madagascar, on 1978. He received, respectively, his M.S degree and PhD in Computer Science and Information Engineering in 2005 and 2008. He served since 2010 as a lecturer at the Higher Institute of Technology Diego Suarez, became an assistant reviewer in 2011. His current research interests include : images compression, multimedia, computer vision, information hiding.

Paul Auguste Randriamitantsoa was was born in 1953. He's a full professor at the Higher Polytehnic School of Antananarivo. His current research interests are : robust control and digital signal processing.