An Invariable to Rotation Data Hiding Scheme for Semi-Fragile Blind Watermark

Khaldi Amine
Computer Science Department, Faculty of Sciences and Technology, Artificial Intelligence and Information Technology Laboratory (LINATI), University of Kasdi Merbah, 30000, Ouargla, Algeria.
khaldi.amine@univ-ouargla.dz

Abstract— **An invariant to rotation watermarking approach is proposed for the purpose of improving the security of digital images. The proposed digital watermark approach is invariable to rotation and guarantees the integrity of the inserted mark. The size of the resulting image is identical to the original image and the process guarantees acceptable transparency. This approach evolves both in the frequency and the spatial domain. Specifically, the proposed scheme processes the JPEG images by adapting its structure to the frequency domain by modifying the DCT coefficients of the image. This scheme is also adaptable to BMP images by adjusting these parameters for an LSB modification of the colorimetric values of the image. Moreover, during the extraction, the structure of our scheme organizes itself according to the orientation of the processed image. Based on the experiment conducting with eight substitution processes, we concluded that the substitution of four bits gives a great capacity of insertion, while guaranteeing an acceptable transparency for the insertion of text. However, a substitution of one bit only is recommended for the insertion of an image. This reduces the capacity, but guarantees transparency of the watermarking process.**

Index Terms—**Digital Image; Digital Watermarking; Frequency Domain; Imperceptibility; Least Significant Bit Substitution; Robustness; Spatial Domain.**

I. Introduction

Following the development of information and communication technologies (ICT), in particular the Internet, which has facilitated the sharing and transfer of digital data [1] through new forms of document hacking, information security is becoming a major challenge. Among these technologies is telemedicine, which allows the sharing and recognition of medical images. In this respect, it is essential to have a security system that protects these images against attacks during the transmission by malicious persons [2]. Encryption techniques are the first solution to prevent unauthorized access to digital data. They meet users' security needs such as confidentiality, integrity and identification. Nevertheless, these techniques have proven to be insufficient or difficult to use [3]. Indeed, cryptographic tools protect the image only during transmission, but once the image is decrypted, there is no control to prevent illegal manipulation. In this context, digital watermarking appears to be an alternative that can be effective and complementary to help establish additional security, ensure authorized access, facilitate authentication of content or prevent illegal reproduction [4]. The idea is to hide an invisible mark in an image (or in a digital multimedia document). A detection or extraction algorithm is required to validate the presence of this mark [5]. In this work, we will propose a digital watermarking approach invariable to the rotation. For this, the images must be marked before the concealment process. This mark should be checked before the extraction process. We must also guarantee the integrity of the inserted mark by calculating a mark hash and inserting it in the image. A modification of the mark will be easily detected by recalculating the hash of the mark and comparing it to that contained in the image. The resulting image should have the same size as the original image to ensure acceptable transparency. We will experiment eight substitution processes to establish the most suitable technique for inserting image or text, taking into account the insertion capacity of each algorithm. The application could evolve by adapting its structure to the spatial and frequency environment. An orientation control allows the algorithm to be adapted to the orientation of the watermarked image when rotated. To ensure the integrity of the mark, this application must also be able to detect any modification of the watermark using a hash algorithm. The remainder of the paper is organized as follows. Section 2 describes the techniques and properties of watermarking as well as the various classifications. In Section 3, we propose our approach of watermarking as well as the results of our experiments, and finally, conclusions from the work is presented and further research is suggested.

II. Digital Watermarking

Digital watermarking involves hiding a signature in a document [6]. This mark, invisible or not, will have characteristics specific to each field of use (robustness, reversibility, capacity and others). Besides taking into considering the intended application and security constraints, watermarking methods must take into account the nature of the data to be processed.

A. General Watermarking Process

Most watermarking algorithms are based on the same model, and they differ only in specific strategies at certain levels of the insertion or detection process. It is therefore, possible to present tattooing images in a generic way. According to Figure 1, the watermarking process can be divided into three main blocks: the block of mark creation insertion, and extraction. The blocks of mark insertion and extraction decide the characteristics of the other blocks and they are the most important ones [7].

Mark extraction phase: According to the design of the algorithm, during this phase one may need the original image. In this case, we refer to an informed watermarking [8]. Otherwise, the watermark is said to be uninformed. In some cases, using an informed watermark can determine if the watermarked image has been attacked.

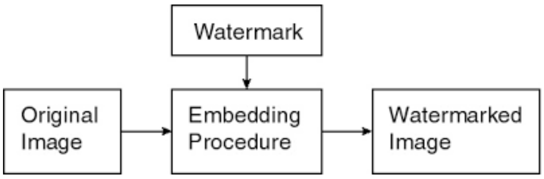

Figure 1: Insertion phase in a watermarking process

B. *Requirements of Digital Watermarking*

In a digital watermark, there are three basic properties, which are intimately linked. These properties are capacity, transparency and robustness [9]. A compromise must be found between these three parameters. Indeed, when we increase the amount of information of the inserted message, we will tend to degrade more strongly the original image or to decrease the strength of the message.

- Capacity: The capacity of the watermarking scheme must also be taken into account. It represents the amount of information that can be inserted. The needs in insertion capacity are not the same according to the purpose of watermarking [10].
- Imperceptibility: Imperceptibility is the fact that the signed image is more or less close, in the visual sense, to the original image. The quality of the watermarked image can also be assessed using tools such as the PSNR. Given the search for mark invisibility, it is important to evaluate the difference in visual perception between the original image and the watermarked image [11].
- Robustness: Robustness represents the ability of the watermark to resist intentional or unintentional alteration of the image and still allow detection of the signature [12]. Robust marking ensures mark protection by resisting manipulations whether malicious or innocent. If the strong mark has been destroyed, this must result in a significant deterioration of the image.

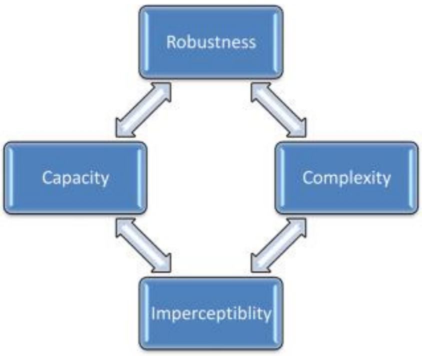

Figure 2: Requirements of digital watermarking

C. *Classification Based on Characteristics*

Blind versus Nonblind: In a blind mode, the receiver has neither knowledge of the watermark nor knowledge of the original image. It is the most interesting method of extraction, but also the most difficult to implement. Conversely, in a nonblind watermarking, the receiver has the image as well as the original watermark [13]. This is incompatible with applications that aim to verify the integrity of the image, or to ensure real-time verification of copyright (problem of access time to the database containing the original information).

Perceptible versus Imperceptible: In a perceptible watermark, the mark is visible in the containing media (a logo for example). In an imperceptible watermark, the embedded watermark must be invisible to the naked eye and could be extracted by a computer [14].

Private versus Public: A watermark is private when only authorized users can detect it. It must ensure that unauthorized users cannot access the watermark. In a public watermark, users can extract the watermark [15].

Robust versus Fragile: Since an image is marked with the W-mark, the W-mark is said to be fragile if its detection fails at the slightest change in the pixels of the image. This mark is considered semi-fragile if its detection fails when the image has undergone a major change or an unacceptable manipulation. It is clear that a fragile mark cannot be robust at the same time since the two constraints are contradictory [16]. Fragile marking algorithms often use hash or digital signature functions.

Spatial Domain Based versus Frequency Domain Based: In the spatial domain, the mark is inserted by directly modifying the values of the pixels of the image. The main advantage of this field is the low computational cost, which allows it to be used in real-time watermarking applications. In the frequency domain, a transform is applied to the image, then the obtained values are used for the integration of the watermark [17]. This transformation allows to control the signal frequencies. It allows to adequately choose the appropriate areas for the insertion of the mark, such as to obtain a good robustness-invisibility compromise. Also, the main advantage of this domain is that it is invariant to translation and scaling.

D. *Applications of Digital Watermarking Images*

The applications of digital watermarking are numerous [18] among the following:

- Authentication of the content of an image: Watermarking is used to check that an image has not been altered. This type of watermarking ensures the integrity of the document. It is used in the authentication of medical images, remote surveillance as well as the security of identity papers. The digital watermarking process consists in hiding information to detect a possible modification or cutting of the image by an unauthorized person and to precisely locate the manipulated areas, or even restore them if necessary.
- Monitor Broadcasts: This application allows content owners or distributors to track the television or Internet broadcast of their content. Watermarking is used to prove that the content has been played in its entirety in generating reports on the state of distribution in a given market at a specific point in time. Additional information may be provided, including conformity of use, as well as license and detection of illegal use [19].
- Copy number control: The objective is to detect the presence of a copyright (a trademark) for the purpose of controlling and making it extremely difficult to copy the work; thus, protecting the rights and benefits of copyright holders. This principle has been used in videos, where the mark indicates whether the video can be copied or not. Indeed, the owner of a DVD has the right to make backup copies, but not to distribute copies to others [20]. Compliant reproduction systems must therefore tolerate first generation copies (made from an original), but prohibit copies of copies. This application

needs the creation of a hardware architecture adapted to the watermarking scheme.

- *Copyright Protection:* Copyright protection was the first application for which the digital watermarking was used. In case of legal conflict, the owner of an image is able to provide proof that he is the owner even if it has suffered damage (attacks). Such an application must ensure a high robustness against attacks, avoid any ambiguity of the proof and minimize the distortions related to the insertion of the mark [21].

III. The Proposed Hiding Scheme (Water_LSB)

In this section we will present the proposed digital watermarking application as well as the tools needed for its realization.

A. *Programming Language*

To implement our application, we used C ++ Builder, which is a compiled programming language that allows programming under multiple paradigms (such as procedural, object-oriented or generic programming). Its good performance and compatibility with C, make it one of the most widely used programming languages for performance-critical applications [22].

B. *Discrete Cosine Transform (DCT)*

The DCT discrete cosine transform was realized in 1974 by Ahmed N and is presented in the article under the title "Image Processing and the Discrete Cosine Transform" [23]. This technique is performed by using image coding to insert the watermark, which makes it more robust to JPEG compression, the most widely used compression among the existing transforms (Figure 3). The advantage of this transformation is to exploit psychovisual methods, which are based on the use of areas where the insertion of the mark remains imperceptible, as opposed to insertion techniques by modifying the coefficients of the DCT. This makes them very fragile to geometrical operations [24].

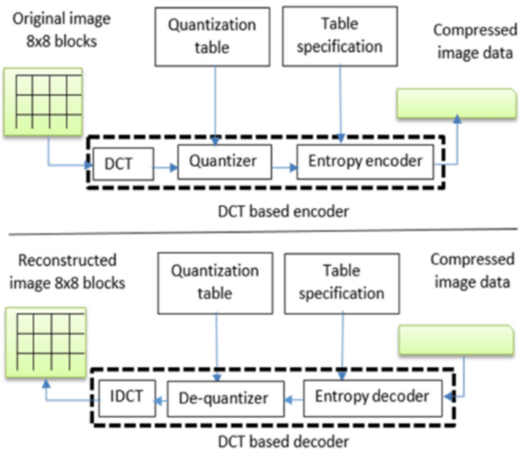

Figure 3: JPEG compression process

C. *Least Significant Bit*

The LSB method involves changing the least significant bit of the pixels encoding the image [25]: A digital image is a sequence of points, called pixels, whose color is encoded using a triplet of bytes, for example for a 24-bit RGB color. Each byte indicates the intensity of the corresponding color red, green or blue (Red Green Blue) by one of 256 levels. Moving from level n to the next higher (n+1) or lower (n-1) level, only slight changes to the hue of the pixel, but this is done by changing the least significant bit in the byte.

D. *Peak Signal to Noise Ratio*

PSNR (Peak Signal to Noise Ratio) is used to determine the imperceptibility of the signature [26]. It allows evaluating the degradation in dB of the original image caused by the insertion of the mark, and possibly by other attacks. When the PSNR is high, the distortion becomes less significant. A watermarking is considered to be imperceptible when the PSNR is greater than 36 dB.

E. *Hash Function MD5*

The MD5, for Message Digest 5, is a cryptographic hash function that provides a digital fingerprint of a file (often referred to as a message). It was invented by Ronald Rivest in 1991. In our work, a hash using MD5 is performed, the resulting binary sequence is then used as a watermark [27].

F. *Watermark Process*

Before the hiding process, the Watermark is hashed using the MD5 algorithm (Figure 4), the generated footprint is added to the Watermark which forms a new Watermark that will be inserted into the image.

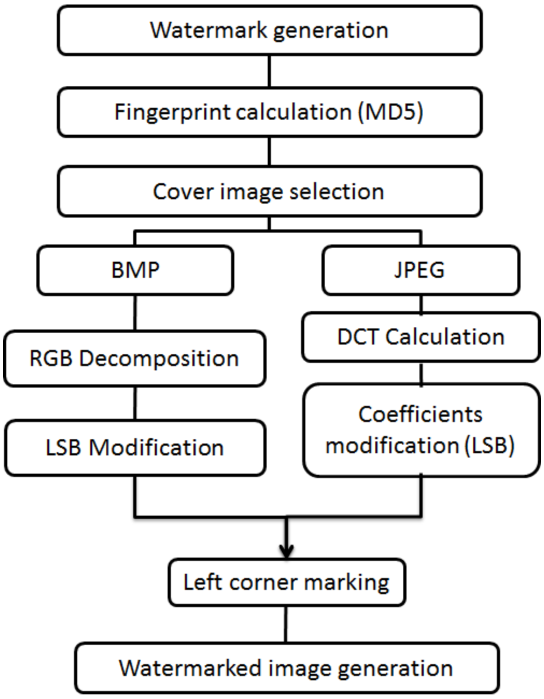

Figure 4: Integration process

In the case of a Bitmap image, the Watermark will be inserted in the low-order bits of the RGB values of the medium cover pixels. In the case of a JPEG image, the image is divided into blocks without overlapping (8*8). Then, for each block, the DCT discrete cosine transform is then applied to anticipate and make the watermark more robust to JPEG compression, since they use the same space that is used to encode the image. Among other things, it reduces the spatial correlation between pixels in an image. Another advantage of using DCT is the possibility to benefit from the psychovisual studies already carried out in source coding.

G. *Experiments and Results*

For our evaluation, we used two image databases used as the cover medium: The first containing 175 bitmap images of equal size (344 kb), and the second is a database of JPEG images of equal size (20 kb). We also used two image databases containing small images (128 * 96 size), one containing JPEG images and the other bitmap. These small images are the watermark that will be inserted into the cover medium. Table 1 describes the possible concealability using the different LSB algorithms from 1 to 8. Substituting a large number of bits for concealment increases the capacity, but the substitution of a lot of bits degrade the image. This is why we must measure the distortion generated by the dissimulation process.

Table 1
Data Hiding Capacity

	Characters	Size (Ko)
LSB1	44032	43
LSB2	88064	86
LSB3	132096	129
LSB4	176128	172
LSB5	220160	215
LSB6	264192	258
LSB7	308224	301
LSB8	352256	344

We used a 1024-character text to mark the images contained in our two image databases, and those with the eight available LSB algorithms. We then calculated the PSNR of 175 marked JPEG images as well as 175 marked Bitmap images. As shown in Table 2, the insertion of the text in the last four bits does not really affect the image too much since the difference of distortion between LSB1 and LSB4 is inferior to 1. We can thus conclude that the use of LSB4 to mark JPEG and BMP images with text without causing significant distortion of the image. We then marked the images of our bases with small images and those with the eight LSB algorithms available. We then calculated the PSNR of the 175 marked JPEG images as well as the 175 marked Bitmap images (Figure 5).

(a) Original image (b) Watermarked image

Figure 5: Example of watermarking using LSB1

Table 2
Imperceptibility Results

	Text Integration		Image Integration	
	BMP	JPEG	BMP	JPEG
LSB 1	64,00	65,37	54,47	59,95
LSB 2	63,95	65,32	50,65	58,16
LSB 3	63,82	65,20	46,23	55,91
LSB 4	63,33	64,81	41,05	53,26
LSB 5	62,15	63,70	36,35	50,41
LSB 6	60,35	62,36	30,28	48,27
LSB 7	54,58	56,22	25,03	41,42
LSB 8	45,70	53,01	16,52	35,40

As shown in Table 2, the distortion increases rapidly when we replace more than one bit in a byte. We can thus conclude that for the marking by inserting images, it is better to use the algorithm LSB1. This will reduce the capacity of the concealment process although it will offer a more reasonable transparency. To compare our application with open source software and free download, we have marked the images of our image databases with 10 watermark applications. We then calculated the PSNR for each image and calculated the average of the 350 results obtained by each software.

Table 3
Image Size after Watermark

Software	PSNR (Db)	Image Size
StegoStick	56,65667	+ 45,25%
OpenStego	56,19667	+0,94%
Steg	55,4	+9,17%
Xiao	55,20333	/
Water_LSB	54,53333	/
Jhide	53,21667	/
Gstegano	51,95667	/
vovsoft	40,74667	+240,65%
PT Watermark	35,13333	/
MTWatermark	31,45	+45,25%
SilentEye	31,05667	/

As shown in Table 3, software like StegoStick and OpenStego generates less distortion than our Water_Lsb application. However, to verify the transparency offered by these software, we also check the sizes of the resulting images. When marking, software such as StegoStick, OpenStego and Steg do not allow having an image identical to the original, StegoStick generates a watermarked image whose size is 45% superior to the original. This is a big problem of transparency especially if you own the original image.

IV. Conclusion

The need for secret or discrete communication is not a new quest: since antiquity, human beings have always sought to protect and disguise their data with different methods. With the advent of the Internet, adapted digital methods were then put in place. In this work, we proposed a watermark approach to mark images in JPEG and BMP formats. The application can evolve by adapting its structure to the spatial and frequency environment. After the calculation of a DCT, the substitution of the bits to be integrated has been performed by modifying the LSBs of the quantized coefficients by comparing the parity of the successive coefficients. Integrating the watermark into the higher coefficients can produce severe distortion of the image, whereas integrating into the lower coefficients makes the watermark robust to compression and filtering. For this purpose, the watermark was integrated using the mid-band coefficients (mixed time and frequency components of the signal) which allowed us to guarantee imperceptibility while being robust to compression attacks and filtering. The use of transforms makes the message more robust to compression, since it uses the same space that is used for image coding. An orientation control allows the algorithm to be adapted to the orientation of the watermarked image when rotated. This application must also be able to detect any modification of the watermark using a hash algorithm guaranteeing the integrity of the mark. The proposed approach guarantees the integrity of the inserted Watermark; a watermark hash is inserted into the image before the hiding process to avoid any integrity problem. A modification of the mark will automatically result in a discrepancy with the hash. After our experiments, we can conclude that a watermark process using text remains reasonably transparent up to four modified bits. However, for the images (which are larger data), the ideal will be to substitute only a bit (least significant) to keep an acceptable transparency. The extension of this work could allow more data concealment and increase the capacity without generating strong distortion of the image.

REFERENCES

[1] Md. Asikuzzaman, Md. Jahangir Alam, Andrew J. Lambert, and Mark R. Pickering, Robust DT CWT-Based DIBR 3D Video Watermarking Using Chrominance Embedding, IEEE Transactions on Multimedia, Volume: 18 , Issue: 9, pp 1733 – 1748, 2016

[2] Franco Frattolillo, Watermarking Protocols: Problems, Challenges and a Possible Solution, The Computer Journal, Volume: 58, Issue: 4, pp 944 – 960, 2015.

[3] Arezou Soltani Panah, Ron Van Schyndel, Timos Sellis, and Elisa Bertino, On the Properties of Non-Media Digital Watermarking: A Review of State of the Art Techniques, IEEE Access, Volume: 4, pp 2670 – 2704, 2016.

[4] Yang Yu, Min Lei, Xiaoming Liu, Zhiguo Qu, and Cheng Wang, Novel zero-watermarking scheme based on DWT-DCT,China Communications, Volume: 13 , Issue: 7, pp 122 – 126, 2016.

[5] Amine Khaldi, Diffie-Hellman Key Exchange through Steganographied Images, Revista de Direito Estado e Telecomunicações, Volume 10, May 2018, Pages 147-160

[6] Dante Mújica-Vargas, José Jesús Rubio, Jean Marie Kinani, and Francisco J. Gallegos-Funes, An efficient nonlinear approach for removing fixed-value impulse noise from grayscale images, Journal of Real-Time Image Processing, Volume: 14, Issue 3, pp 617-633, 2018

[7] Jose de Jesus Rubio, Diana M. Vázquez, and Dante Mújica-Vargas, Acquisition system and approximation of brain signals, IET Science, Measurement & Technology, Volume: 7, No. 4, pp 232-239, 2013

[8] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption, IEEE Access, Volume: 6, pp 19876 – 19897, 2018.

[9] Dante Mújica-Vargas, Francisco J. Gallegos Funes, Jose de Jesus Rubio, and Jaime Pacheco, Impulsive noise filtering using a median redescending m-estimator, Intelligent Data Analysis, Volume: 21, No. 3, pp. 739-754, 2017

[10] Jose de Jesus Rubio, SOFMLS: online self-organizing fuzzy modified least-squares network, IEEE Transactions on Fuzzy Systems, Volume: 17, No. 6, pp. 1296-1309, 2009

[11] Mehran Andalibi, and Damon M. Chandler, Digital Image Watermarking via Adaptive Logo Texturization, IEEE Transactions on Image Processing, Volume: 24, Issue: 12, pp 5060 – 5073, 2015.

[12] F.Kahlessenane, A.Khaldi, and S.Euschi, A robust blind color image watermarking based on Fourier transform domain, Optik, Volume 208, April 2020

[13] Min-Jae Hwang, JeeSok Lee, MiSuk Lee, and Hong-Goo Kang, SVD-Based Adaptive QIM Watermarking on Stereo Audio Signals, IEEE Transactions on Multimedia, Volume: 20, Issue: 1, pp 45 – 54, 2018.

[14] Baharak Ahmaderaghi, Fatih Kurugollu, Jesus Martinez Del Rincon, and Ahmed Bouridane, Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory, IEEE Transactions on Computational Imaging, Volume: 4, Issue: 1, pp 46 – 59, 2018.

[15] Amine Khaldi, A lossless blind image data hiding scheme for semi-fragile image watermark, International Journal of Computational Vision and Robotics, 2020, DOI: 10.1504/IJCVR.2020.10029218

[16] Deepayan Bhowmik, Matthew Oakes, and Charith Abhayaratne, Visual Attention-Based Image Watermarking, IEEE Access, Volume: 4, pp 8002 – 8018, 2016

[17] Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, and Guolin Hou, Secure and Robust Fragile Watermarking Scheme for Medical Images, IEEE Access, Volume: 6, pp 10269 – 10278, 2018

[18] Amine Khaldi, Steganographic Techniques Classification According to Image Format, International Annals of Science, Volume 8, 2019, Pages 143-149

[19] Liancheng Zhang, Yazhou Kong, Yi Goo, Juwei Yan, and Zhenxing Wang, Survey on network flow watermarking: model, interferences, applications, technologies and security, IET Communications, Volume: 12, Issue: 14, pp 1639 – 1648, 2018

[20] A. Sengupta, and S. Bhadauria, Intellectual property core protection of control data flow graphs using robust watermarking during behavioural synthesis based on user resource constraint and loop unrolling factor, Electronics Letters, Volume: 52 , Issue: 6, pp 439 – 441, 2016

[21] Shuai Liu, Zheng Pan, and Houbing Song, Digital image watermarking method based on DCT and fractal encoding, IET Image Processing, Volume: 11 , Issue: 10, pp 815 – 821, 2017

[22] Ferda Ernawan and Muhammad Nomani Kabir, A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold, IEEE Access, Volume: 6, pp 20464 – 20480, 2018

[23] Weiqing Wang, Junyong Ye, Tongqing Wang, and Weifu Wang, Reversible data hiding scheme based on significant-bit-difference expansion, IET Image Processing, Volume: 11 , Issue: 11, pp 1002 – 1014, 2017

[24] Abbas Najafipour; Abbas Babaee, and S. Mohammad Shahrtash, Comparing the trustworthiness of signal-to-noise ratio and peak signal-to-noise ratio in processing noisy partial discharge signals, IET Science, Measurement & Technology, Volume: 7, Issue: 2, pp 112 – 118, 2013

[25] Zhenguo Gao, Danjie Chen, Wei Zhang, and Shaobin Cai, Colour image encryption algorithm using one-time key and FrFT, IET Image Processing, Volume: 12, Issue: 4, pp 472 – 478, 2018

[26] Jong-Uk Hou, Do-Gon Kim, and Heung-Kyu Lee, Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact, IEEE Transactions on Information Forensics and Security, Volume: 12, Issue: 11, pp 2712 – 2725, 2017

[27] Xiao-Long Liu, Chia-Chen Lin, and Shyan-Ming Yuan, Blind Dual Watermarking for Color Images' Authentication and Copyright Protection, IEEE Transactions on Circuits and Systems for Video Technology, Volume: 28 , Issue: 5, pp 1047 – 1055, 2018