INTELLIGENT SIGNAL PROCESSING

OVERVIEW AND CLASSIFICATION OF DIGITAL WATERMARKING ALGORITHMS

Predrag Milosav[1, 2, *],
Zoran Banjac[2],
Milan Milosavljević[1],
Tomislav Unkašević[1, 2]
Medhat Abdelrahman
Mohamed Mostafa[3]

[1]Singidunum University,
Belgrade, Serbia
[2]Vlatacom Institute,
Belgrade, Serbia
[3]European University,
Belgrade, Serbia

Abstract:
This paper performs a comparative analysis of different watermarking techniques. Namely, in the last twenty-five years, a large number of algorithms for digital watermarking have been developed. In order to understand how different schemes can be applied it is important to define some criteria for classifying them. The algorithms are classified according to the characteristics of embedded watermarks and based on applications in which the watermark is built in. The robustness of the watermarks with respect to a different kind of attacks is also analyzed.

Keywords:
Watermark, Image Processing, Robustness, Data Embedding.

1. INTRODUCTION

Digital watermark is commonly used in the field of information security, copyright protection, data authentication, and broadcast control. The watermark is embedded in the carrier, which can be audio, video or other data, in such a way that the distortion caused by the embedding is too small to be noticed. At the same time, the embedded watermark must be sufficiently reliable and robust to withstand conventional degradation, alterations or deliberate attacks. In addition, for acceptable levels of distortion and robustness, the desire is to incorporate as much data as possible in a particular carrier and thus increase its capacity. Podilchuk and Delp presented a general framework for the embedding and detection / decoding of watermarks [1], taking into account their differences in their implementations and in different watermark algorithms and applications in the context of copyright. In the following section, the WM algorithm will be presented in the first chapter by basic characteristics and by the place of application. The second chapter will explain the basic techniques of embedding the watermark into different types of carriers. The third chapter is reserved for advanced watermarking techniques in order to solve the problems brought with the basic techniques mentioned in the second chapter. The last chapter is reserved for the conclusion of the complete work.

Correspondence:
Predrag Milosav

e-mail:
predrag.milosav@vlatacom.com

DOI: 10.15308/Sinteza-2019-537-545

2. CLASSIFICATION IN DIGITAL WATERMARKING

Digital watermarking technology has been developed as a convenient tool for identifying sources, creators, owners, distributors or an authorized consumer of the document or digital content. It can also be used to identify and track data illegally distributed. There are two main steps in the digital watermark process: (1) embedding the watermark in which the watermark is inserted into the content of the carrier, and (2) extracting the watermark, in which the watermark is extracted from the carrier. Nowadays there are a number of algorithms for imprinting watermarks. It is important to define some criteria for their description and classification in order to understand how different schemes can be applied.

Classification based on characteristics

This section categorizes digital watermarking technologies into five classes according to the behavior and characteristics of embedded watermarks.

Blind versus nonblind - The watermarking technique is considered to be *blind* if it does not require access to the original carriers, without watermark (video, images, sound, etc.), to restore the watermark. On the other hand, the watermark technique is considered *nonblind* if the original carrier is required to extract a watermark. Watermarks can be extracted using several different algorithms, Barni and Nikolaidis belong to the blind category, and on the other hand, Cox and Swanson algorithms belong to the nonblind [2-5]. Using of blind or nonblind algorithm are tradeoff robustness and complexity of use.

Perceptible versus imperceptible - A perceptible watermark is embedded and foreseen to be visible, usually by the author. A perceptible watermark is considered good if it is made so that it is difficult to remove and change by an unauthorized person, as well as that it can resist counterfeiting. On the other hand, imperceptible watermark is embedded with a sophisticated algorithm and made to be invisible to the user. However, it can be extracted using an inverse algorithm, only by the owner or authorized user.

Private versus public - A good quality watermark is considered *private* if only authorized users can detect and extract it, and such techniques have been developed to prevent unauthorized users to alter it or remove it (for example, using a private encryption key). This set of data stores information about the watermark location in the carrier, allowing the insertion or removal of a watermark if some of the links in that communication chain are compromised. On the other hand, public watermarks are embedded in a location that is well known to everyone and can be easily accessed and easily extracted. Basically, private watermark techniques are more robust than public, in which an attacker can easily remove, alter or damage data when the embedded code is known. A special type of public watermark is an asymmetric type in which each user can read a watermark without the ability to change, damage or remove it. Similar to asymmetric cryptography systems, the private key is used to incorporate a watermark and the public key is used for WM verification.

Robust versus fragile - The robustness of the watermark is reflected in the ability of a watermark to survive a legitimate daily use or manipulation by digital processing, such as intentional or unintentional attacks. The targets of the deliberate attack are to destroy or damage the watermark, while unintentional attacks do not explicitly intend to change it. According to the robust characteristics, watermarks can be categorized into three types: *Robust, Semifragile and Fragile.*

Robust watermarks have been designed to survive deliberate and unintentional modifications of the watermark carrier [3,4,6,7]. Inappropriate tendencial changes include the unauthorized removal or modification of the embedded watermark as well as the malicious insertion of any other information. Unintentional modifications include image processing operations such as scaling, cropping, filtering, and compression. In order to preserve information on ownership rights, robust watermarks are usually used to protect copyrights.

Semifragile watermarks have been developed to detect any attempt of unauthorized modification, while allowing some image processing operations [8]. This type of watermark technique can distinguish common image processing and content-preserving noise such as impulsive noise, lossy compression or bit error from malicious content modifications.

Fragile watermarks were developed to detect any unauthorized modifications [9-13]. This type of watermark refers to the complete verification of origin and integrity, so that the smallest intentional or accidental modification of the carrier with the watermark will change or destroy the watermark. It's mainly used for authentication purposes.

Spatial domain based versus frequency domain based - There are two image domains for embedding watermarks: spatial domain and frequency domain. In the

spatial domain [14], the watermark can be inserted into the carrier by changing the gray level of some pixels of the original gray-scale carriers or pixels values in each color (RGB) channel for full color carriers. This method has the advantages of low complexity, simple implementation and low processing power needed, but the inserted information can easily be detected by computer analysis or can be easily attacked and altered. The watermark can be embedded into the coefficient of transformed image in the frequency domain [4,15]. Transformations include *discrete cosine transformation*, discrete Fourier *transform*, and *discrete wavelet transformation*. If too much data is embedded into the carrier in the frequency domain, the image quality will be significantly decreased. Spatial domain watermark techniques are usually less resistant to attacks such as compression and additional noise. However, they have a much lower computational complexity and can usually survive a cropping attack, whose watermark technique often does not succeed in the frequency domain. Another technique is the combination of watermarking of the spatial domain and a watermark of the frequency domain to increase robustness and obtain less complexity.

Classification based on application

This section categorizes digital watermarking technologies into five sections according to the following usage and applications:

Copyright protection - The idea of this kind of protection is that watermarks are invisibly inserted into a carrier that can be detected when the product of the process (output file or stream) is compared with the original. They are designed to unambiguously identify the source of the carrier, origin and its authorized users. Identification of ownership and recipients by the technique of inserting an invisible watermark attracted great interest in the printing and publishing industry. The idea of copyright protection on a digital video is the incorporation of a watermark into a video stream that transmits information about the sender and receiver and the whole process is considered more critical when delivering digital content compared to the broadcasting of analogue signals. This watermark method can enable the identification and tracking of different copies of video data.

Data authentication - According to this scenario, the watermark can be considered a handwritten signature of a document and provides a high degree of protection. By comparing the two signed documents it can be ascertained whether they were created by the same person. The user signs the digital document using his private key, which is strictly intended for this need by his mathematical and cryptographic characteristics. Digital signatures can be checked using a public key according to the principles of asymmetric cryptography, in which two keys are used that are mutually related mathematically. To all who want to perform the verification, the public key as well as the verification methodology are available.

Fingerprinting - Checking digital documents requires some reliable methods that can undoubtedly prove the authenticity of the document. Following the uniqueness of biometric characteristics in the context of human distinction, a similar principle of fingerprinting was applied to digital documents. Digital fingerprints in the form of a watermark can be applied to protect digital content from malicious attacks, detect fake and counterfeit digital content and ensure secure transmission. This allows the copyright owner to track a pirate if the digital content is abused or distributed illegally. The content of a watermark that has the role of a fingerprint is an identification number that is unique to each content user, with the goal of establishing authenticity as well as a possible source of illegally distributed copies. Such watermarks must be additionally protected by cryptographic methods.

Copy control - The main idea was to protect copyright content in digital format from illegal copying and multiplication. In the case of DVD technology, it is clearly shown how the copy control information, indicating the copying level, is added to the main data, recorded on the digital recording medium, so that the master data comprises a first part containing the image and / or voice information, and the second part containing copy control information. The digital watermark is embedded in the second part of the master data and in combination with the first part of the data provides protection against illegal copying of digital content.

Device control - Device control watermarks are embedded control access to a resource using a special verification system. The watermark with the role of the authorization code is embedded in the signal and transmitted (for example, as a television or radio program) to the verification device. For the purposes of remote control of an apparatus such as a toy, computer or device, identical technique using watermarks may be applied. A device that has the role of recognizing the existence of a watermark is equipped with a suitable detector to identify hidden signals that can trigger an action or change the state of the device. An excellent example of the application of such a technology is a system that

automatically recognizes the broadcast of paid advertisements on the media, so that the ordinary listener does not notice the existence of a hidden watermark that is only visible to systems that are set to recognize it.

3. DIGITAL WATERMARKING FUNDAMENTALS

In accordance with the classification described in the previous chapter, the basic techniques of embedding of digital watermarks will be presented in detail below. Each of these techniques is based on the appropriate idea, then the mathematical basics, the modes of implementation, the complexity of the model, the challenges of successful watermark extraction, and the degree of resistance to different types of attacks. Depending on the aforementioned characteristics of each of the techniques, a suitable application will be mentioned and proposed.

Substitutive Watermarking in the Spatial Domain - The substitutive watermarking in the spatial domain is the basic and simplest watermark algorithm [11,17]. Locations for embedding, such as specific pixel bits, whether in gray-scale or in color image, are pre-defined before embedding a watermark. When the recipient receives a watermark image, they know the exact locations as well as the corresponding number of bits from which the watermark can be extracted.

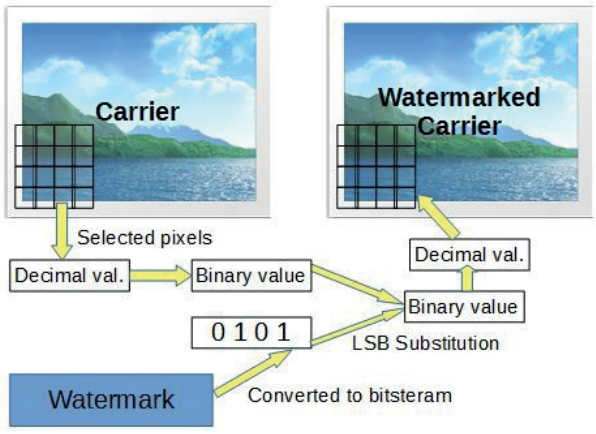

Fig 1. The substitutive watermarking embedding procedure in the spatial domain

Figure 1 shows the watermarking algorithm in the gray-scale carrier, while Figure 2 shows the reverse operation, in particular process of extracting the embedded watermark In general, the capacity of the watermark in the spatial domain is greater than the other watermark access. If the watermark is embedded in three LSBs, human beings usually can't distinguish the original image from a watermarked image. With the increase in the number of modified bits, the carrier capacity is increased, but also degrades carrier characteristics. The substitutive watermarking is easy to implement and does not require a high processing power or a large processing time. The embedded watermark is not robust against collage or lossy compression attack. For this reason, some improved spatial watermarking algorithms for enhancing robustness are proposed - for example, the hash function method and the bipolar M-sequence method [9, 11].

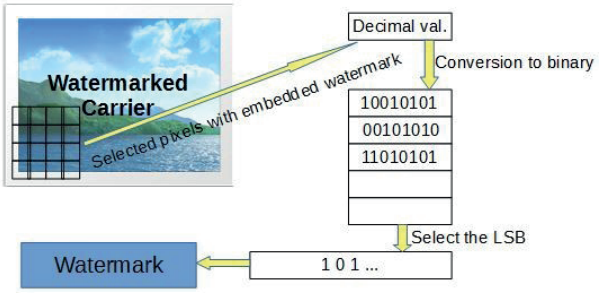

Fig 2. The watermark extracting procedure of substitutive watermarking in the spatial domain

Additive Watermarking in the Spatial Domain - Starting from the idea where the specific bits of certain pixels are not taken, the additive watermark technique has been developed. Instead of the precisely defined bits of certain pixels, only part of the watermark value in the pixel is added to perform the embedding process. If H is the original grayscale host image and W is the binary watermark image, then {h (i ,j)} and {w (i ,j)} denote their respective pixels. We can embed W into H to obtain the watermarked image H* as follows:

$$h^*(i,j) = h(i,j) + a(i,j) \cdot w(i,j) \quad (1)$$

where {a (i ,j)} denotes the scaling factor.

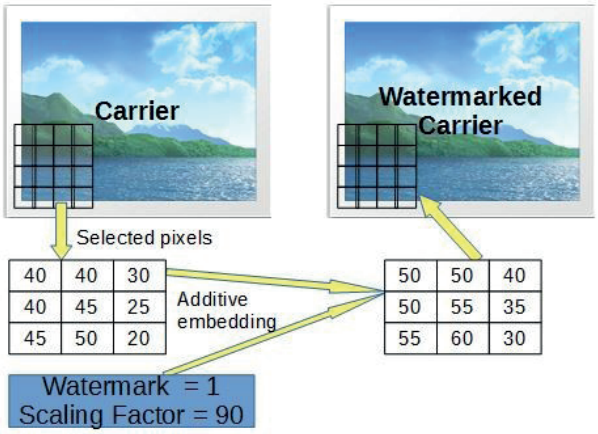

Fig 3. Method of block-based additive watermarking in the spatial domain

With the aim to enhance imperceptibility, a big value is not embedded to a single pixel, but into a dedicated block of pixels [18,19]. Figure 3. shows an example of the block-based additive watermarking. First, a 3 × 3 block is selected for embedding a watermark while the scaling factor will be 90. Second, the amount of scaling factor is divided by 9 (matrix size). Even the scaling factor is quite large, the decimal value of the pixels has not been changed too much so that when a recipient obtains the watermarked image, it is difficult to determine the embedded message since he does not know the location of the block for embedding. By this approach, we increased the robustness of the watermarked data, increased its resistance to different types of attacks and at the cost of reducing the capacity of the carrier. It is also important to select the proper value of the scaling factor according to the type of carrier and the used application of the additive watermarking.

Substitutive Watermarking in the Frequency Domain - In the frequency (or spectral) domain watermarking [6, 20], we can insert the watermark into the frequency coefficient of the image if it is previously transformed by discrete Fourier transform (DFT), discrete cosine transformation (DCT) or discrete wavelet transformation (DWT). The scheme of the substitution watermark in the frequency domain is basically similar to that of the spatial domain, except that the watermark is embedded in the frequency coefficients of the transformed carrier. The spatial coefficients of the watermarked image are obtained by inverse transformation as shown in Figure 4. By changing the specific coefficients in the frequency domain, we made a change in the corresponding number of decimal values of the pixels in the spatial domain. Such changes will adequately affect the quality and robustness of the watermarked image.

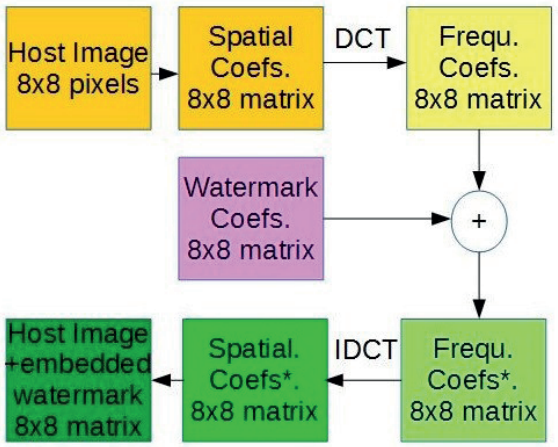

Fig 4. Algorithm of Substitutive Watermarking in the Frequency Domain

Multiplicative Watermarking in the Frequency Domain – The main idea of this method is that the watermark is scaled to the value of a specific frequency component of the transformed carrier. If H is the DCT coefficients of the carrier image and W is the random vector, then {h(m ,n)} and {w(i)} denote their respective pixels. We can embed W into H to become the watermarked image H* as follows:

$$h^*(m,n) = h(m,n)(1+\alpha(i)\cdot w(i)) \tag{2}$$

The magnitude of distortion of the watermarked image depends on the scaling factor *{α (i)}* value. It is usually set to be $0 < \alpha(i) < 1$ to provide a good trade-off between imperceptibility and robustness. An alternative embedding formula using the logarithm of the original coefficients is as follows:

$$h^*(m,n) = h(m,n)\cdot e^{\alpha(i)\cdot w(i)} \tag{3}$$

The watermark can be extracted using the inverse embedding formula, as follows:

$$w'(i) = \frac{h^*(m,n) - h(m,n)}{\alpha(i)\cdot h(m,n)} \tag{4}$$

Watermarking Based on Vector Quantization – Main idea is lossy block-based compression technique in which

vectors, instead of scalars, are quantized. Each partitioned, 2D block of pixels, maps to a final set of vectors that form a codebook that must be unique for the encoder and decoder. On the receiving side, calculation similar to cross-correlation of the vector is performed, and then the index of the vector that best fits the input block is sent to the decoder. A codebook is used to store all the vectors, their sizes and positions. For every input vector v, Euclidean distance is calculated in the search process to measure the distance between two vectors, as follows:

$$k = \arg\min_j \sqrt{\sum_i (v(i) - s_j(i))^2} \quad (5)$$

where $j = 0, 1, \ldots, N-1$. The closest Euclidean distance code word s_k is selected and transmitted to the decoder. With the same codebook, the decomposition procedure can easily extract the vector v via lookup table. Lu and Sun developed basics of the image-watermarking technique based on VQ [21]. During their proof of concept, codebook was divided into a few clusters of close code vectors with the Euclidean distance less than a given threshold. The model requires the original image for watermark extraction and the secret key was actually a part of the codebook. During the research they came to the conclusion that a tampering attack is detected if the received index is not in the same cluster as the best-match index.

Fragile Watermarks - Fragile watermarks represent a methodology and a means of ensuring that a received image can be trusted. Hidden fragile watermark will be evaluated by the recipient to see whether the image has been altered. Therefore, the fragile watermarking technique is used to detect any unauthorized modification. *Block-Based* fragile watermarks are very good described in Wong's watermarking insertion algorithm. Figure 5. shows the process of embedding a portion of the watermark W_r obtained by partitioning the watermark W, into a part of the carrier X_r obtained by dividing the carrier X. Figure 6. shows an inverse process, or the extraction of a part of the watermark E_r.

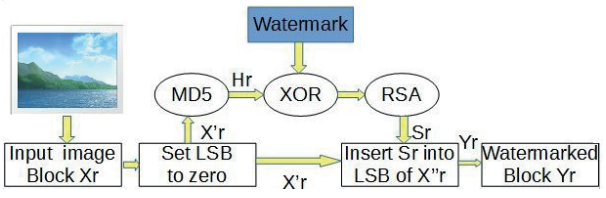

Fig 5. Wong's watermarking algorithm for data insertion

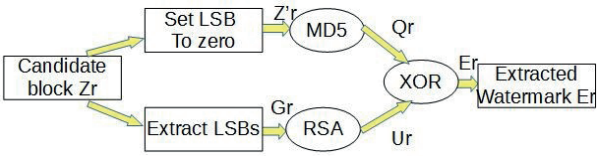

Fig 6. Wong's watermarking extraction algorithm

The idea of *Hierarchy-Based* watermarking approach is completely opposite to Wong's algorithm and it is based on breakdown of block independency. Because of the main idea of the method, it comes to the conclusion that the technique is good to defeat a VQ counterfeiting attack. Due to linking blocks to a larger entities, the embedded data not only include the information of the particular block but also possess the relative information of the higher-level blocks from the same entity. Just because of that, a VQ attack cannot estimate or recognize an image based on a codebook that only keep the information of each watermarked block.

Robust Watermarks - Robust watermarking is well chosen technique for providing security for copyright protection, which ensures that the embedded messages can survive attacks such as JPEG compression, Gaussian noise, and low-pass filtering. In order to advance robustness, *Redudant Embedding Approach* is one of the possible techniques and it's described by Epstein and McDermott patent for copy protection [22]. Cox algorithm have presented a *Spread Spectrum* – based robust watermarking algorithm in which the embedded messages are spread throughout the image [4,15]. Main idea is that the watermark is embedded in significant coefficients of host image, in frequency domain, transformed by DCT. In this way, the percent value of the significant coefficients will be the least affected.

4. ADVANCED TECHNIQUES OF DIGITAL WATERMARKING

Combinational Domain Digital Watermarking

The idea of high-capacity watermarks is minimizing image distortion while simultaneously increasing the amount of data that can be stored in the carrier. The presented technique involves combining the embedding of information in the spatial and frequency domain at the same time. The scenario is based on watermark splitting into two parts used for spatial and frequency

insertions, depending on the characteristics of the carrier, user preferences and the importance of the data. A carefully selected splitting strategy can be designed to be very complicated to make it unbeatable. Using random watermarking permutations increases robustness in order to better protect against image processing attacks such as cropping. The question is, how to insert more signals, but to keep the visual effects unperceivable? The main idea is to divide the watermark W into 2 parts, W1 and W2; to embed W1 into the spatial domain image H of the host and get H^S; then to embed W2 in the frequency domain of the host H^{DCT} domain to obtain the H^F; then execute IDCT in H^F and superpose it with H^S. The processing result will be a data of the carrier with an embedded watermark based on the combination algorithm for the watermark.

WM Based on Genetic Algorithms

Genetic algorithms, introduced by Hollard, are commonly used as adaptive approaches for providing randomized, parallel, and global search mechanisms based on natural selection and genetic principles in order to find solutions to the problem. The method is developed to improve retrieving of a noisy watermark from watermarked image if LSB substitution approach utilized as the embedding strategy and the watermark is embedded in frequency domain. Main challenge is prediction what the impacts will be in the frequency domain of a cover image if changes are made to the values of pixels in the spatial domain. GAs are considered to be the best method for solving the problem. By changing the pixel in the frequency domain, it is difficult to intuitively conclude what will happen to coefficients in a spatial domain. It is difficult to determine whether the embedded data in the frequency domain is of significance or not in the process of translating real numbers into integers. On the other hand, it's also difficult to predict how to change the corresponding pixels in order to avoid errors and to perform correct data embedding. It is therefore not only difficult to intuitively select the coefficients to be changed, but it is also very likely that such changes will lead to a very poor result. In order to solve previous problems, GA is used as an appropriate solution for rounding real numbers into integers instead of the traditional rounding approach. As GA is based on the chromosome model, reproduction, crossover and mutations, on similar principles, the theory applied in the process of embedding and extraction of watermarks.

Adjusted-Purpose Watermarking

Previous approaches have shown that all watermarking techniques are divided according two features: watermarking purpose (robust or fragile) and domain watermarking algorithm (spatial or frequency). Knowing this we are concerned with two primary issues:

1. How to adjust the approach to performing watermarking from the spatial to frequency domain?
2. How to adjust the purpose of watermarking from fragile to robust?

There are few different approaches in Adjusted Purpose Watermarking techniques:

A *morphological approach* to extracting the pixel-based (PB) features. Mathematical morphology, based on the theory of sets, can recognize the characteristics of the object by selecting a suitable structure and then perform an analysis of the selected structure and conclude on the success of a particular iteration. The analysis is of a geometric character and attempts to bring approach to the characteristics of human perception. Morphological operators deal with two images. The image being processed is referred to as the active image, and the other image, being a model. By designing and classifying different forms of structuring, it is possible to simplify the presentation of image data and explore the characteristics of shapes.

Some methods are based on selection and adjusting the variable-sized transform window (VSTW) and Quantity Factor (QF). According to two developed parameters VSTW and QF different techniques will be performed. Scenario consider watermarking in spatial domain when the VSWT=1x1 and in the frequency domain for other sizes. On the other hand, by adjusting the value of the QF, the embedded watermarks will become robust if the QF is large and become fragile if the QF is 1.

Reversibile Watermarking

Previous chapters shows that most existing fragile watermarking schemes usually makes some permanent distortions in the original image for embedding the watermark information. However, for some multimedia specific applications, such as medical diagnosis, law enforcement, and fine art, the generated distortions are not allowed. For solving that problem there are two kind of reversible data-hiding schemes proposed.

First proposed scheme is based on chaotic fragile watermarking technique. This approach consider difference of two neighboring pixels, their average values are calculated and the secret data that have to be embedded are appended to a difference value and represented as a binary number. Further, using the histogram of the pixels in the carrier image to design a reversible hiding scheme, where the pixels between the peak and zero are modified in the embedding process and the pixel in the peak point of histogram is used to carry a piece of the secret message. Proposed algorithm obtain the chaotic hash value of each image block that is computed as the watermark, which ensures that complicated nonlinear and sensitive dependence within the image' s gray features, secret key, and watermark - exists. The huge size of the key space is very important and beneficial for image authentication. Moreover, after the authentication message has been extracted, reversible watermark embedding allows the exact recovery of the original image.

Second proposed scheme is based on techniques using multiple scan difference-value histogram modification. Two metrics parameters that describe performance are important to consider with a reversible data-hiding technique. The first is the maximum payload, which is the maximum amount of data that can be embedded into an image. The second is visual quality, which is measured using the PSNR (peak signal to noise rations) between the original image and the image with embedded watermark. Three different scanning techniques are used for the construction of the difference histograms in order to maximize the payload capacity. The scanning techniques that we use are horizontal, vertical, and diagonal. Adjacent pixels are more likely to have similar values and according to this the scanning order is very important, so the result in a difference histogram that has most of its values near zero.

5. CONCLUSION

By classifying and reviewing the digital watermarking techniques, their mathematical and implementation models, as well as reviewing their specific purposes and suitable sites for use, a clear picture is obtained of the application possibilities as well as a better basic position for further analysis and improvement of implementation. It is clear that there is no universal watermark technique that will satisfy all application needs while being both simple to implement, quick to perform and resistant to various types of attacks. On the other hand, the good quality knowledge and understanding of the digital watermarking technique provides an opportunity for infinite research and improvement of existing methods of embedding, extraction and application of watermarks as well as techniques of steganography as a related scientific discipline.

REFERENCES

[1] C. Podilchuk and E. Delp, "Digital watermarking: algorithms and applications", *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33–46, 2001.

[2] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking", *Signal Processing*, vol. 66, no. 3, pp. 357–372, 1998..

[3] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain", *Signal Processing*, vol. 66, no. 3, pp. 385–403, 1998.

[4] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[5] Swanson, M. D., Zhu, B., and Tewfik, A. H., "Transparent robust image watermarking", in *Proc. IEEE Int. Conf . Image Processing*, Lausanne, Switzerland, 1996, 211

[6] S. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415–421, 2000.

[7] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack", *Signal Processing*, vol. 83, no. 10, pp. 2133–2170, 2003.

[8] Sun, Q. and Chang, S.-F., "Semi-fragile image authentication using generic wavelet domain features and ECC", in *Proc. IEEE Int. Conf. Image Processing*, 2002, 901.

[9] P. W. Wong, "A public key watermark for image verification and authentication", *Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No.98CB36269).*

[10] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization", *IEEE Transactions on Image Processing*, vol. 11, no. 6, pp. 585–595, 2002.

[11] R. Wolfgang and E. Delp, "A watermarking technique for digital imagery: Further studies", in *Proc. Int. Conf. Imaging Science, Systems and Technology*, Las Vegas, NV, 1997, 279.

[12] I. Pitas and T. Kaskalis, "Applying signatures on digital images", in *Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, 1995, 460.

[13] G. Caronni, "Assuring Ownership Rights for Digital Images", *Verläßliche IT-Systeme*, pp. 251–263, 1995.

[14] H. Berghel and L. Ogorman, "Protecting ownership rights through digital watermarking", *Computer*, vol. 29, no. 7, pp. 101–103, 1996.

[15] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video", *Proceedings of 3rd IEEE International Conference on Image Processing*., 1996, 243.

[16] W. G. Chambers, "Basics of Communications and Coding", *Oxford Science*, Clarendon Press, Oxford, 1985.

[17] F. Y. Shih and S. Y. Wu, "Combinational image watermarking in the spatial and frequency domains", *Pattern Recognition*, vol. 36, no. 4, pp. 969–975, 2003.

[18] E. T. Lin and E. J. D. Iii, "Spatial synchronization using watermark key structure", *Security, Steganography, and Watermarking of Multimedia Contents VI*, 2004.

[19] D. Mukherjee, S. Maitra, and S. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 1–15, 2004.

[20] J. Huang, Y. Shi, and Y. Shi, "Embedding image watermarks in dc components", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 6, pp. 974–979, 2000.

[21] Z. Lu and S. Sun, "Digital image watermarking technique based on vector quantisation", *Electronics Letters*, vol. 36, no. 4, p. 303, 2000.

[22] M. Epstein and R. McDermott, "Copy protection via redundant watermark encoding", USA Patent no. 7133534, 2006, accessed on January 5, 2017, http://www.patentgenius.com/patent/7133534.html