A STUDY ON MULTIPURPOSE WATERMARKING TECHNIQUES FOR IMAGE

Nidaa Hasan Abbas[1] Sharifah Mumtazah Syed Ahmad[1,2]Sajida Parveen[1.]
Wan Azizun Wan Adnan[1] abd. Rahman Bin Ramli[1]
[1]Department of Computer and Communication System Engineering,, Faculty of Engineering, Universiti Putra Malaysia,Serdang, Selangor D. A. 43400.
[2] Research Centre of Excellence for Wireless and Photonics Network (WiPNET), Universiti Putra Malaysia. Serdang, Selangor D. A. 43400.
Contact: nidaahasan71@gmail.com

ABSTRACT *Conventional single watermark systems are mainly aimed at accomplishing a single goal, either for forgery detection or image copyright protection. This limitation has resulted in the introduction of multipurpose or otherwise known as multifunction watermarking algorithms, with the prime objective of simultaneously achieving both goals. Research in this domain has attracted tremendous interest in recent years, mainly due to its challenging nature in effectively satisfying both aims without degrading one another. However, most of the recent studies have not indicated a clear distinction between multipurpose and multiple watermarks (or cocktail watermarking) algorithms.*

This paper differentiates between these two types of digital watermarking systems and focuses on multipurpose watermarking due to its significance. In addition, it presents a state of the art survey on the theories, models, features, and algorithms that have been implemented in designing a multipurpose watermarking algorithm. It highlights the recent trends in related techniques and most reliable results attained, whilst also pointing the possible future research directions that can be investigated.

Keywords Digital Watermarking; Robust Watermark; Fragile Watermark; Multiple watermarks; Multipurpose watermarking system.

1. INTRODUCTION

With the huge development in digital media and the rising use of internet, digital media products are increasingly exposed to a number of threats. Amongst of which are unauthorized duplications and distributions of digital media over the internet [1] .

The traditional cryptography protection strategy has its limitation, as it does not track digital products against illegal reproductions after they have been decrypted. This has led to the need of digital watermarking techniques that provide effective detection mechanisms for copyright protection. For such purpose, the embedded watermark must be robust and resistive towards deliberate attacks. However, conventional watermarks for copyright protection are often incapable of media tampering detection, which makes them ineffective for content authentication [2].

Content tampering or counterfeiting is another increasing threat to digital media. For instance, the numerous availability of image editing software packages has given novice users the ability to modify or manipulate the content of digital products. Thus, it is also somewhat essential to embed watermarks for integrity detection [3]. Especially, on critical digital media such as those used for news reporting, medical archiving, and forensic evidences. Cryptographic signatures have only the ability to protect media from tampering while they remain encrypted. However, once decrypted the media becomes vulnerable to illegal modification and cryptography techniques are incapable of highlighting any compromised items.

Watermarks which are used for tampering detection do not require the same robustness level as those used for copyright protection. This is mainly because it needs the ability to detect even the slightest modification to the media. The two contradictory requirements are a great challenge in designing a multipurpose watermarking algorithm. Therefore, based on this, most digital watermarking systems perform a single task, either for copyright protection or tampering detection. However, high-valued applications such as military satellite images require both objectives to be satisfied simultaneously. Therefore, developing a double function watermarking system is a critical requirement. Thus, with regard to robustness, an acceptable level of compromise is desirable. Two situations can be identified: the watermark can either be fragile, indicating that any small alteration, or semi-fragile, allowing an acceptable level of alterations such as slight contrast adjustment or low-level lossy compression in images [4].

In this paper, a survey on multipurpose watermarking systems is presented, with particular concern on the significant advancements in image watermarking, as well as, the differences between multipurpose and multiwatermarks algorithms. To the best of our knowledge, there is currently no related literature that has presented such review. The rest of the paper is organized as follows:

Section 2 presents the concept of multiple watermarks systems and their differences with the multipurpose watermarking. Section 3 describes the principles of multipurpose watermarks systems, their classification, and provides a review of the available algorithms. Evaluation of performance of the algorithms is explained in section 4. Section 5 reports the most promising research trends along with the conclusions of this paper.

2. Multiple watermark systems

The differences between multipurpose watermarking and multiple watermark systems should be addressed [5] , [6]. This is because there is currently no significant study concerned with distinguishing the two techniques, only a short discussion was provided in [5] and [6]. In Multiple watermark, two or more robust watermarks are mainly employed for copyright protection. Each one being designed to bear certain types of attacks such as the algorithm proposed by [7] which employed a second invisible watermark to back up the first visible one and increase the robustness of the system against cropping attack. The multiple watermark methods are frequently used in visible watermarking. The main requirements for visible watermarking algorithms are: the watermark should be recognizable, unobtrusive, and difficult to remove. The last

requirement is the most required from the commercial point of view. Although there are many attempts to develop this property, still visible watermarking algorithms are vulnerable to inpainting attack; which means removing the embedded watermark [8,9]. It is difficult to design a visible watermarking scheme to fulfill all aforementioned requirements. Furthermore, a visible watermark being robustly designed may be tampered by the means of various software. Developing an algorithm to detect such kind of tampering (in worst case to protect the image when the visible watermark is fully removed) has become a critical issue. Based on this, researchers have employed multiple watermark algorithms that utilize an invisible watermark to back-up the visible watermark such as the techniques proposed in [19,11]. The two studies implemented the embedding process in the spatial domain. Mohanty *et al*. [10] embedded invisible watermark as authentication code in the most significant bit (MSB) of the watermarked image that contains a visible logo. Wong *et al*. [11] embedded the two watermarks in the spatial domain of the host image. They improved the security by combining both cryptography function and public key. This system is computationally expensive and not suitable for most practical applications because of public key usage [12].

Additionally, in situations whereby the visible watermark is attacked by any means, the invisible authentication code can be retrieved to verify whether the image has been tampered or not, without indicating the ownership of the watermarked image. In this regard, many approaches such as [12 , 13] and [14] have been developed to compensate the shortcomings of the techniques proposed in [10,11] by embedding the invisible watermark in the frequency coefficients of a visibly watermarked image using discrete wavelet transform (DWT). DWT is one of the most computationally efficient multi-resolution frequency transform that utilizes the human visual system (HVS). The invisible watermark in these cases can be extracted and used as a proof of ownership for protected image when the visible watermark is removed. The scheme in [12] is robust to JPEG compression and can partially resist inpainting attack which is a critical attack in case of visible watermarking design. In the algorithm proposed by [13], both host and primary watermark image were decomposed into two resolution levels using Daubechies-4 filter. The secondary watermark was added to the horizontal coefficients of the decomposed primary watermark image. The resulting watermark coefficients were then added to the horizontal, vertical, and diagonal DWT sub-bands of the original host image. A constant scaling factor α was used to adjust the invisibility of the watermark. This work was modified in [14] using an adaptive scaling factor instead of the constant one . The adaptation of α was adjusted depending on the energy content of the image to be watermarked. This modification enhanced the Peak Signal to Noise Ratio(PSNR) by about 10 dB. However, there are interference between the two watermarks in [10–14] and the latter watermark must modify the values of the former pixel so the former watermark suffers from serious distortion without any attack. In addition, these algorithms are unable to bear the inpainting and malicious processing attacks [15].

The weaknesses were handled by the work presented in [15]. The ownership of the image can be indicated by means of the visible watermark and the invisible watermark can protect the image from malicious attacks. The authors used mixed domains for embedding the two watermarks. Frequency domain was utilized for the invisible watermark based on DCT, while the visible watermark was embedded in the spatial domain. The subsampling techniques employed by [16,17 was adopted to simultaneously hide the watermarks without affecting each other. In addition, they preprocessed the image to increase the robustness using chaotic function performed by [18] and the just noticeable difference (JND). However, the methodology of the algorithm is more complicated [19] and still vulnerable to some attacks such as compression and geometric attack as the spatial and DCT domains are vulnerable to such kinds of attacks [20]. The authors in [20] exploited these points in designing their systems and embedded three biometric watermarks using wavelet packet transform. They embedded two invisible biometric

watermarks; owner's speech and Gabor face to protect the third visible watermark which is offline signature. The Gabor face is embedded in the wavelet packet coefficients of the host image. The selection of the subbands used for embedding had been performed according to the empirical values of PSNR of the retrieved Gabor face. The second stage of biometric embedding includes embedding the speech watermark after being compressed by Linear Predictive Coding (LPC) in the horizontal sunbband of the wavelet. Finally, the offline signature was overlaid visibly on the watermarked image. The interference among the three watermarks was avoided by making embedding stages independent of each other. In addition, each watermark can be extracted individually at each stage or from the final watermarked image. However, the computational complexity of the system is high. Also, the robustness was tested against a limited number of attacks and some critical attacks such as geometric attacks were not taken into account.

Substantially, the main requirements for multiple watermark or cocktail watermark algorithms include robustness to intentional and non-intentional attacks, computationally efficient and the two watermarks should be non overlapped. It is worth mentioning that designing a multiple watermark algorithm that satisfies the aforementioned requirements is still an open area of research.

3. Multipurpose watermarking algorithms

The scenario here is different to the multiple watermark algorithms, as multipurpose watermarking algorithms basically require embedding two different watermarks within the same media which are collectively aimed at achieving different objectives; copyright protection and tampering detection [28]. There are several restrictions involved in embedding them. Firstly, both techniques should not interfere with one another, and secondly, the embedding order of the two watermarks.

Mintzer and Braudaway [21] suggested to embed the robust watermark first and the fragile one later, because the robust watermark has the ability to resist various types of transformations (intentional and unintentional) to a certain

extent and the fragile watermark is highly susceptible to small changes [22, 23] .

In this study, multipurpose watermark systems are classified from a more general perspective into two schemes with respect to the priority principle of embedding order. In scheme (1), the two watermarks (the robust and the fragile watermarks) are embedded in sequence one after the other. While in scheme (2), the two watermarks are embedded simultaneously. By this classification, some disadvantages of Chen and Shen.'s classification [24] is introduced. They classified the multipurpose watermarking into three schemes. In scheme (1), the two watermarks are merged and considered as one watermark. While in scheme (2), embedding the two watermarks is done in sequence, one after the other, and for scheme (3) the two watermarks are embedded simultaneously. But, it is worth noting that all the works that belong to scheme (1) are not real multipurpose watermarking as claimed, but they were merely multiple watermarks for one mission (copyright protection).

3.1 Scheme (1)

In this method, the embedding process of two watermarks is performed consecutively one after the other. Fig.1 shows this scheme. As suggested by Mintzer and Braudaway [21], the ownership protection watermark should be cast first, then the less sensitive watermark for image authentication is embedded. Consequently, the order of extraction should follow the inverse order, hence from fragile to robust watermark.

Most researchers adopt this scheme in performing the multipurpose watermark systems because the two watermarks can be embedded dynamically. Example is the work proposed by [25] in which the embedding and retrieving processes had been performed in wavelet transform. The work had been tested against various attacks; JPEG compression, geometric and nongeometric. In addition, all the watermarked images had been detected and recovered after had been tampered so it achieves copyright protection and image authentication and recovery simultaneously. The procedure of embedding is as follows: two different watermarks were used for authentication and recovery image simultaneously; the first watermark is image feature extracted from the original image and the second one is logo image. They first partitioned the original image into non overlapped blocks. DWT was applied to these blocks; the low frequency subband of each block was extracted and used as image feature to represent the first watermark. The watermark was embedded into the corresponding block to accomplish image authentication and recovery at the same time. To embed the second watermark for copyright protection, it was embedded in the middle frequency subband. Despite the algorithm performing the multipurpose watermark successively, it is obvious that the computational complexity of the algorithm is high.

Another important multi-resolution transform that has been used recently in image watermarking is the Contourlet Transform (CT). CT is more effective than wavelet transform in capturing edges and smooth contours in images.

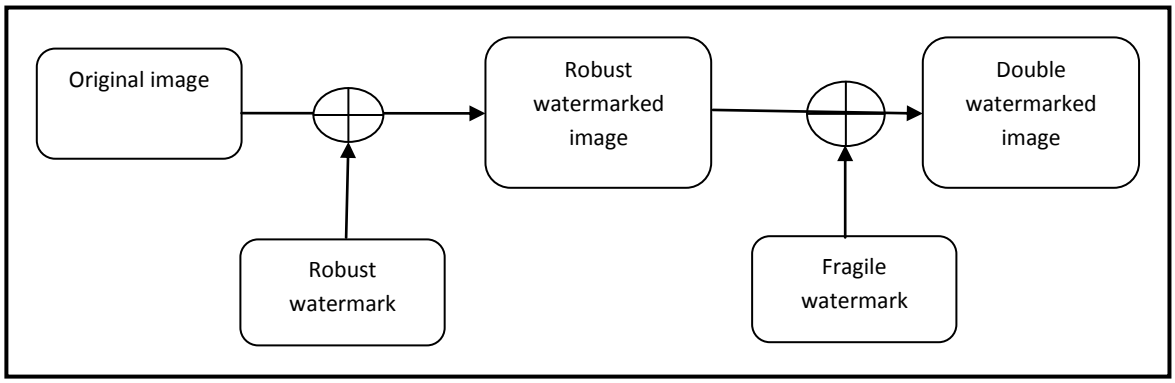

Fig.1 Multipurpose watermark embedding scheme (1)

performed in the lowpass subbands . However, the invisibility may be enhanced if the embedding process is carried out in the detail subbands of CT [27].

The work proposed by [26] employed this transform in embedding the dual watermarks into region of interest(ROI) and region of noninterest (RONI). The system was designed for digital imaging and communications in medicine (DICOM). The embedding process was

Recently, many researchers have tried to develop watermarking systems by combining both spatial and transform domains to compensate the drawback of each other, for example the works proposed by [28,29]. In the algorithm proposed by [28], the original image is decomposed by DWT and the coefficients are quantized and hashed using secure cryptographic hash functions. The second watermark was added to the encrtypted coefficients using dither modulation [30] to decrease the embedding visual distortion. While the first watermark was hidden imperceptibly in the spatial domain. In this way, the second watermark should not interfere with the watermark previously embedded in the spatial domain. The algorithm can withstand JPEG and JPEG2000 compression since the second watermark was embedded in the DWT domain of JPEG2000, and also it can resist geometric attack like compression and scaling. On the other hand, in [29] the robust watermark was embedded in the spatial domain, whereas the fragile watermark was embedded in the DCT domain of the host video signal. Although the system can

resist certain attacks and detect image manipulation, but still suffers from block artifacts introduced by DCT [31] .

Some approaches have been proven to be effective against many attacks, but they are computationally expensive like the works proposed by [32,33] . The authors in [32] embedded the robust watermark in the intermediate frequency coefficients of the singular value decomposition (SVD) and Distributed Discrete Wavelet Transform (DDWT) of the host image. Then, the fragile watermark was adapted and embedded in the spatial domain of the host image. The system was tested against many attacks and had proven to be robust. However, no test was performed to prove the system's fragility. In [33], the host image was first decomposed into M self-fractional Fourier function (SFFF) images, and then these images were further decomposed into intrinsic mode functions (IMFs) by means of bivariate empirical mode decomposition (BiEMD). The robust watermark was also encoded using error correcting code before embedding into the residue signal resulting from BiEMD of SFFF images. The fragile watermark was self generated from the host image to achieve self authentication, but in the experimental results there is no evidence for achievng this purpose.

Many lossless dual functions schemes have been proposed such as [34,35,36]. The best nominees amongst them is the system proposed by [36] this system combining the watermarking system with a security mechanism to avoid multiple claims of rightful ownership. They utilized vector quantization (VQ) together with cryptographic tools to get better reliable and secure system. The VQ is used to encode the watermark and index set is produced which in turn would be signed by the owner of the private key with a digital signature. Then, the signed index set is further time-stamped protection, image by a trusty certification authority (CA) for certification purpose. However, this scheme had achieved robustness at the expense of fragility. According to [37] the schemes that based on conventional VQ in selecting the embedded coefficients have a high computational complexity because VQ needs designing a code book to be transmitted from the transmitter side to the receiver side. This point has been seriously excited by [37,38]. A novel multipurpose watermarking scheme was presented by [37] based on DWT and chaotic map. Improvement quantization method (IQM) was used to embed the binary watermark in the host image effectively. In designing IQM scheme, there are two quantization parameters Q and q as shown in Fig.(2). In embedding the robust watermark, the majority bit value b (b=0 or b=1) is selected by scanning original binary watermark sequence W_R. Embedding was performed according to the watermark bit w; the DWT coefficient f of the host image was forced to the nearest range f [kQ-q, kQ+q], if the embedding watermark w is the majority bit value b and if the embedding watermark w is 1-b, then f was forced to the nearest value (k+1/2)Q , here, k=0,±1,±2,…. The fragile watermark Fw which was a chaotic sequence iterated 1000 times. The iterated map was converted into 0 or 1 according to quantization function q (·) to obtain Fw (i, j)=0,1. Then the preprocessed fragile watermark was embedded into randomly selected coefficients from LH (i, j) , 2HL (i, j) , 2HH (i, j) subbands of the decomposed original image according to odd-even quantization process. Another system that improved the vector quantization is the system proposed by [38] based on Blind Vector Quantization (BVQ) that performs copyright

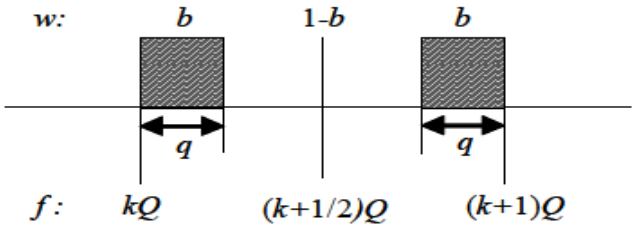

Fig. 2 The improvement quantization method

authentication and distinguishing between malicious and non-malicious manipulations. With BVQ mechanism no need for codebooks to be transmitted to the receiver side, so the transmitting performance was improved as compared to traditional vector quantization. The robust watermark was scrambled with a key and separated into two equal parts; w_{emd} was embedded into LL subband of the decomposed image after adjusting the coefficients according to w_{emd} while the other part w_{key} was transmitted to the receiver side as a secret key. The fragile information that used for image verification is generated by the sender to the receiver using the well-known Linde-Buzo-Gray (LBG) algorithm.

Most of multipurpose watermarking systems illustrated above did not deal with copy attack, in which unauthorized user can copy a watermark from one document to another, making these documents in question in all authentication applications. The authors in [39] handled this issue by proposing a multipurpose watermarking system that employs a highly robust watermark and a fragile/semi-fragile watermark for copyright protection, tamper-proofing, and robust to copy attack. The fragile watermark based on local hash-codes and embedded in a way which fully preserves the robust part; in the LSB of selected pixels to firstly ensure less perceptual distortions and secondly, these selected positions do not contain the robust watermark.

3.2 Scheme (2)

Embedding the two watermarks according to scheme (1) is impracticable in real applications [53] so many authors [40,41,44,45] employed scheme (2) in embedding the two watermarks simultaneously rather than consequently as in Fig.3.

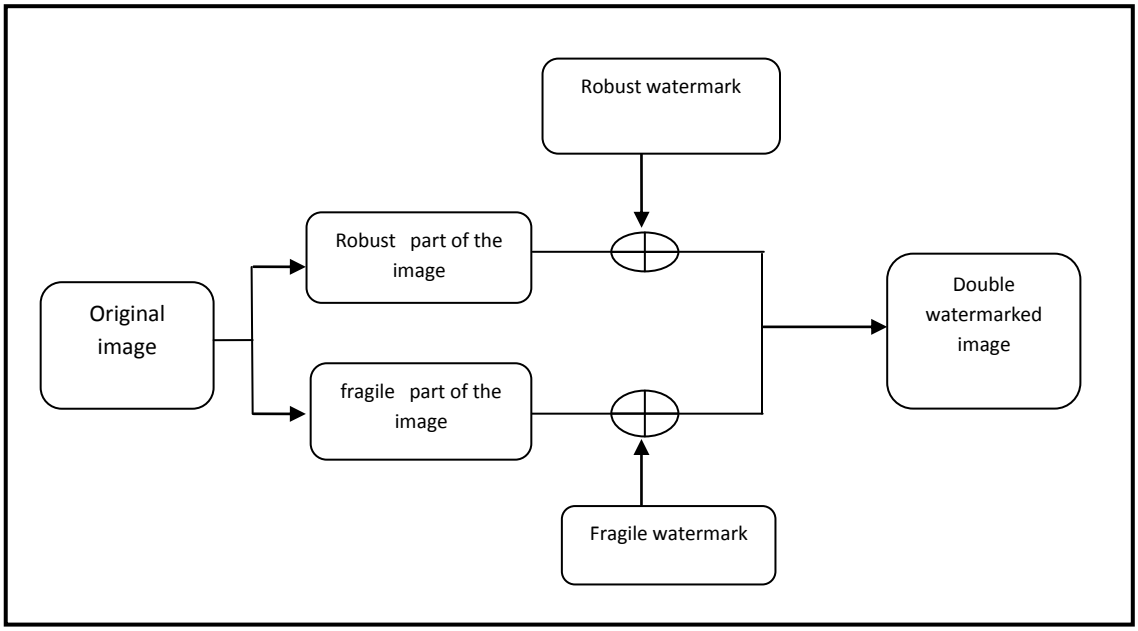

Fig.3 Multipurpose watermark embedding scheme (2)

The aim of this scheme is to solve the ordering problem of scheme (1) by decomposing the image into two components so the two watermarks can be embedded with no interference and the characteristics of each watermark can be preserved [53].

There are few works that adopted this scheme such as the works proposed by [40,41]. The two algorithms were implemented in DCT. The fragile and robust watermarks in [40] were embedded into two different color components of the color image at the same time. The robust watermark was embedded in the G component of the color image. The G component was divided into 64 × 64 blocks and decomposed by DCT. The relationship between middle frequency DCT coefficients and the DC component was modified according to the value of watermark bits. The robust watermark fulfilled the requirements, but the time required for embedding was high as the watermark was repeated for every block of DCT. Embedding the fragile watermark was performed in spatial domain using LSB [42], cryptography and lossless compression. As in the robust watermark, the B component of the color image is divided into 64 × 64 blocks. (MD5) technique employed by [43] was used to encrypt each block and lossless compression was performed using a Huffman code. It is obvious that fragile watermark embedding was repeated for every block so the embedding time was high as in the robust watermark. In general, most watermarking systems that hide the watermark in the DCT domain of the host image truncate or round off the DCT coefficients to the nearest integer and ignore the decimal part to increase the robustness of the algorithms . This process will result in loss of imperceptible details. The proposed system by [41] took this point into consideration and no truncation was implemented to the DCT coefficients; consequently, the system became less lossy.

Another approaches that embedded two watermarks simultaneously are [44,45] were implemented in the wavelet domain. The image was decomposed by means of DWT and the selected coefficients were quantized as masking threshold units. The two watermarks were embedded by modulating the quantization result into either a right or a left masking threshold unit using cocktail watermarking [5]. The robust algorithm that employed cocktail watermarking can resist many attacks excepting geometric attacks [46,47,48]. The system fragility was investigated and the manipulation was detected. The authors in [45] extended the single robust algorithm proposed by [49] and [50] into a double function watermark algorithm for copyright protection and image authentication. They used the improved pixel-wise masking model employed by [51] and bit substitution based on pseudo-random sequence proposed by [52] to hide the robust watermark and the fragile watermark into insensitive and sensitive part of the wavelet coefficients respectively. By this way, they reduced the interference between the two watermarks. But the watermarked image has some perceptual artifacts and the algorithm had subjected to only noise, filtering and JPEG attacks and the geometric attacks were not handled.

Two works presented by [57,52] that succeeded in avoiding the interference between the two watermarks however their systems have a storage capacity problem [53]. Lu *et al*. [51] employed multistage vector quantization to decompose the original image into two components; one approximation for embedding the robust watermark and residual components for semifragile watermark embedding. This system required high storage capacity as five secret matrices should be stored and transmitted to be used by the decoder side as secret keys. Chang *et al.*'s system [52] has the same storage problem as the XOR results between the robust watermark and the wavelet coefficients of the original image needs to be stored for verification [53].

Most existing multipurpose watermarking used two watermarks for the two purposes, while [53] suggested to achieve the two purposes of copyright protection and content authentication without considering two watermarks embedding. The authentication watermark was derived from the lowpass curvelet coefficients while the embedding was controlled by the key from the copyright holder.

In spite embedding two watermarks, fragile and robust according to scheme (2) has solved the problem of avoiding the interference between the two watermarks , the embedding has some considerations that should be taken into account during the embedding and retrieving stages since the two watermarks are embedded at the same time into two different components of the original image and this may explain why the scheme has been used quite sparingly.

4. Evaluating multipurpose watermarking algorithms

As mentioned previously that avoiding interference between the two watermarks and embedding order are the main constraints that should be taken into account in designing a multipurpose algorithm. However, evaluation of each algorithm should be performed according to the achieved features for both robustness and fragility. The desirable features for robust watermark are its ability to resist various types of attacks while for fragile watermark are its ability to detect with high probability any pixel manipulation in a watermarked image [54] . In addition, some authors claimed that their schemes have achieved two functions, copyright protection, and image authentication. But from the experimental results, it is obvious that only one function has been achieved. In this regard, Table 1 highlights the evaluation of the algorithms based on the robustness, fragility, and the ability to perform multifunction.

Table (1) : Evaluation of the multipurpose algorithm (G=good, M=medium,W=weak, Y=yes,N=no)

Algorithms	Scheme	Operating domain	Robustness	Fragility		Ensure interference	Perform multipurpose
				Detect	Localize		
[25]	1	DWT	G	Y	Y	N	Y
[26]	1	CT	G	N	N	Y	N
[28]	1	Mixed	G	N	N	Y	N
[29]	1	Mixed	M	Y	N	Y	Y
[32]	1	Mixed	G	N	N	Y	N
[33]	1	Mixed	G	N	N	N	N
[34]	1	Mixed	M	N	N	Y	N
[35]	1	Mixed	G	N	N	Y	N
[36]	1	Mixed	M	N	N	N	N
[37]	1	Mixed	M	Y	Y	Y	Y
[38]	1	Mixed	G	Y	Y	Y	Y
[39]	1	Spatial	G	Y	Y	Y	Y
[40]	2	Mixed	M	Y	Y	Y	Y
[41]	2	DCT	G	N	N	N	N
[44]	2	DWT	M	Y	Y	N	Y
[45]	2	DWT	M	Y	Y	Y	Y
[51]	2	Vector	G	N	N	Y	N
[52]	2	DWT	M	N	N	Y	N
[53]	2	Curvelet	M	N	N	Y	N

5. CONCLUSION AND FUTURE WORK

The multipurpose or multifunction system is a new challenging area of research in digital watermarking. It mainly focuses on combining dual watermarks; robust and fragile to achieve content authentication and also copyright protection. However, most of the recent studies have not indicated a clear distinction between multipurpose and multiple watermarks (or cocktail watermarking) algorithms which the latter is primarily employed for only copyright protection by embedding multiple robust watermarks. So in

this survey the differences between them are highlighted and introduced a detailed discussion of multipurpose algorithms which are mainly divided into two schemes depending on the sequence of embedding the two watermarks. Evaluation of multipurpose algorithms has been performed according to the achieved features for both robustness and fragility and the ability to perform multifunction.

There are still future researches that can be done on multipurpose watermarking systems. The following are the suggestions for future works.

- Focus on the two missions; robustness and fragility.
- Ensuring no interferences will occur between the two watermarks.
- Designing algorithm that can withstand some attacks that affect critically on the purpose of the algorithm since the previous proposed schemes were designed to withstand only certain kinds of attacks.

Minimizing the time of watermarks embedding and extraction and reducing the computational complexities of the algorithm since most researchers give attention only to the robustness and fragility for their algorithms

REFERENCES

1. Xi Zhao: Robust and Semi-fragile Watermarking Techniques for Image Content Protection. M. Phil/PhD Transfer Report. (2009).
2. Yuan, H., Zhang, X.-P.: Multiscale fragile watermarking based on the Gaussian mixture model. IEEE Trans. Image Process. 15, 3189–200 (2006).
3. Friedman, G.L.: The trustworthy digital camera: restoring credibility to the photographic image. IEEE Trans. Consum. Electr. 905–910 (1993).
4. M.M. Yeung, F.C.M.: An invisible watermarking technique for image verifcation. In: Image Processing (ICIP '97). pp. 680–683 (1997).
5. Lu, C.-S., Huang, S.-K., Sze, C.-J., Liao, H.-Y.M.: Cocktail watermarking for digital image protection. Multimedia, IEEE Trans. 2, 209–224 (2000).
6. Busch, C., Wolthusen, S.D.: Tracing data diffusion in industrial research with robust watermarking. In: Multimedia Signal Processing, 2001 IEEE Fourth Workshop on. pp. 207–212. IEEE (2001).
7. Shih, F.Y., Wu, S.Y.T.: Combinational image watermarking in the spatial and frequency domains. Pattern Recognit. 36, 969–975 (2003).
8. Huang, C.-H., Wu, J.-L.: Attacking visible watermarking schemes. Multimedia, IEEE Trans. 6, 16–30 (2004).
9. Pei, S.-C., Zeng, Y.-C.: A novel image recovery algorithm for visible watermarked images. Inf. Forensics Secur. IEEE Trans. 1, 543–550 (2006).
10. Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.: A dual watermarking technique for images. In: Proceedings of the seventh ACM international conference on Multimedia (Part 2). pp. 49–51. ACM (1999).
11. Wong, P.W., Memon, N.: Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans. Image Process. 10, 1593–601 (2001).
12. Hu, Y., Kwong, S., Huang, J.: Using Invisible Watermarks to Protect Visiblywatermarked Images. In: IEEE International Symposium on Circuits and Systems. pp. 584–587 (2004).
13. Sharkas, M., Elshafie, D., Hamdy, N., IEEE, S.M.: A Dual Digital-Image Watermarking Technique. World Acad. Sci. Eng. Technol. 5, 136–139 (2005).
14. ElShafie, D.R., Sharkas, M., Hamdy, N.: An Energy-Based Dual Image Watermarking Technique with Application to Color Images. 2006 49th IEEE Int. Midwest Symp. Circuits Syst. 602–605 (2006).
15. Lin, P., Lee, J., Chang, C.: Dual Digital Watermarking for Internet Media Based on Hybrid Strategies. IEEE Trans. Circuits Syst. Video Technol. 19, 1169–1177 (2009).
16. Chu, W.C.: DCT-based image watermarking using subsampling,. IEEE Trans. Multimed. 5, 34–38 (2003).
17. Lu, W., Lu, H., Chung, F.-L.: Robust digital image watermarking based on subsampling. Appl. Math. Comput. 181, 886–893 (2006).
18. Shih, Y.T.W. and Y.: Digital watermarking based on chaotic map and reference register,. Pattern Recognit. 40, 3753–3763 (2007).
19. Lin, P.-Y.: Imperceptible visible watermarking based on postcamera histogram operation. J. Syst. Softw. 95, 194–208 (2014).
20. Inamdar, V.S., Rege, P.P.: Dual watermarking technique with multiple biometric watermarks. Sadhana, 39, 3–26 (2014).
21. Mintzer, F., Braudaway, G.W.: If one watermark is good, are more better? In: Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on. pp. 2067–2069. IEEE (1999).
22. Gabor, D.: Theory of communication. Part 1: The analysis of information. J. Inst. Electr. Eng. III Radio Commun. Eng. 93, 429–441 (1946).
23. Furon, T., Duhamel, P.: Robustness of asymmetric watermarking technique. In: Image Processing, 2000. Proceedings. 2000 International Conference on. pp. 21–24. IEEE (2000).
24. Chen, B., Shen, H.: A New Robust-Fragile Double Image Watermarking Algorithm. 2009 Third Int. Conf. Multimed. Ubiquitous Eng. 153–157 (2009).
25. Wang, L., Syue, M.: A Wavelet-based Multipurpose Watermarking for Image Authentication and Recovery. 2, 100–108 (2013).
26. Rahimi, F., Rabbani, H.: A dual adaptive watermarking scheme in contourlet domain for DICOM images. Biomed. Eng. Online. 10, 53 (2011).
27. Haohao, S.: Contourlet based adaptive watermarking for color images. IEICE Trans. Inf. Syst. 92, 2171–2174 (2009).
28. Schlauweg, M., Pröfrock, D., Zeibich, B., Müller, E.: Dual watermarking for protection of rightful ownership and secure image authentication. Proc. 4th ACM Int. Work. Contents Prot. Secur. - MCPS '06. 59 (2006).
29. Moon, S.-W., Kim, H.-D., Lee, J., Lee, H.-K.: Dual video watermarking for CCL protection and manipulation detection. 2012 IEEE Int. Symp. Circuits Syst. 1420–1423 (2012).

30. Schlauweg, M., Pröfrock, D., Palfner, T., Müller, E.: Quantization-based semi-fragile public-key watermarking for secure image authentication. In: Optics & Photonics 2005. p. 591506. International Society for Optics and Photonics (2005).
31. Kaur, R., Brar, G.S.: Reduction of Blocking Compression Artifacts.
32. Yang, H., Zhang, T.: A New Algorithm of Compound Image Watermarking Based on DDWT. In: 2008 International Conference on MultiMedia and Information Technology. pp. 268–271. Ieee (2008).
33. Sharma, J.B., Sharma, K.K., Sahula, V.: Digital image dual watermarking using self-fractional fourier functions, bivariate empirical mode decomposition and error correcting code. J. Opt. 42, 214–227 (2013).
34. Shieh, C.-S., Huang, H.-C., Wang, F.-H., Pan, J.-S.: An embedding algorithm for multiple watermarks. In: Journal of information Science and engineering. Citeseer (2003).
35. Wong, P.H.W., Au, O.C., Yeung, Y.M.: Novel blind multiple watermarking technique for images. Circuits Syst. Video Technol. IEEE Trans. 13, 813–830 (2003).
36. Huang, H.-C., Feng-Hsing, W., Jeng-Shyang, P.A.N.: A VQ-based robust multi-watermarking algorithm. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 85, 1719–1726 (2002).
37. Zhu, C., Hu, Y.: A Multipurpose Watermarking Scheme for Image Authentication and Copyright Protection. 2008 Int. Symp. Electron. Commer. Secur. 930–933 (2008).
38. Lin, C.: Multipurpose Watermarking Based on Blind Vector Quantization (BVQ). 2, (2011).
39. Deguillaume, F., Voloshynovskiy, S., Pun, T.: Secure hybrid robust watermarking resistant against tampering and copy attack. Signal Processing. 83, 2133–2170 (2003).
40. Jun, Y., Guo-Hua, C., Yi-jia, Z.: A practical multipurpose color image watermarking algorithm for copyright protection and image authentication. In: Digital Telecommunications, 2006. ICDT'06. International Conference on. p. 72. IEEE (2006).
41. Habib, M., Sarhan, S., Rajab, L.: A Robust-Fragile Dual Watermarking System in the DCT Domain. 548–553 (2005).
42. S Walton.:Information Authentication for a Slippery New Age [J]. Dr Dobbs J. 20, 18–26 (1995).
43. Schneier, B.: Applied Cryptography, 1996. Cover title pages. 125–147.
44. Liao, H.-Y.M.: Multipurpose watermarking for image authentication and protection. IEEE Trans. Image Process. 10, 1579–1592 (2001).
45. Shen, H., Chen, B.: From single watermark to dual watermark: A new approach for image watermarking. Comput. Electr. Eng. 38, 1310–1324 (2012).
46. Kutter, M.: Watermarking resistance to translation, rotation, and scaling. In: Photonics East (ISAM, VVDC, IEMB). pp. 423–431. International Society for Optics and Photonics (1999).
47. Pereira, S., Pun, T.: Fast robust template matching for affine resistant image watermarks. In: Information Hiding. pp. 199–210. Springer (2000).
48. Ruanaidh, J.J.K., Pun, T.: Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Processing. 66, 303–317 (1998).
49. Xie, G., Shen, H.: Toward improved wavelet-based watermarking using the pixel-wise masking model. In: Image Processing, 2005. ICIP 2005. IEEE International Conference on. pp. I–689. IEEE (2005).
50. Gui, X.I.E., Hong, S.: A new fusion based blind logo-watermarking algorithm. IEICE Trans. Inf. Syst. 89, 1173–1180 (2006).
51. Lu, Z.-M., Xu, D.-G., Sun, S.-H.: Multipurpose image watermarking algorithm based on multistage vector quantization. Image Process. IEEE Trans. 14, 822–831 (2005).
52. Chang, C.-C., Tai, W.-L., Lin, C.-C.: A multipurpose wavelet-based image watermarking. In: null. pp. 70–73. IEEE (2006).
53. Zhang, C., Cheng, L.L., Qiu, Z., Cheng, L.-M.: Multipurpose watermarking based on multiscale curvelet transform. Inf. Forensics Secur. IEEE Trans. 3, 611–619 (2008).
54. Lin, E., Delp, E., Lin, E.T., Delp, E.J.: A Review of Fragile Image Watermarks. (2001). In Proc. 1st Int. Conf. Innovative Computing, Information and Control, 2006, vol. 3, pp. 70–73.