Digital Images Watermarking Using Hybrid Algorithm

Kulveen Singh¹ and B S Dhaliwal²

Guru Kashi University E-mail: kulveen.singh@gmail.com

Abstract—Security and authentication of knowledge are important problems to be thought-about. a great deal of analysis goes on to extend security and authentication. During this thesis we tend to be giving a brand new image watermarking methodology. During this paper prime focus is will increase the safety and authentication by embedding multiple watermarks within the image while not reducing the standard of the image. To infix a watermark victimization DWT-DCT-Viterbi, info embedded is convolution encoded 1st. Given a rate R"k/n convolution code, the N info bits square measure divided in teams of N/k symbols that square measure consecutive introduced within the convolutional encoder. The cryptography of data of watermark before embedding will increase security.

Keywords: Watermarking, Digital Security, Spatial Embedding, LSB, DCT.

1. INTRODUCTION

1.1 Need of Watermarking

Digital image process could be a speedily developing space with varied raising applications in engineering science and engineering. It's important field for the analysis work as a result of its techniques are utilized in most varieties of work like human computer interface, medical visualization; image improvement, enforcement, creative effects, image reconstruction and watermarking for security concern. Digital image process has several useful properties over the analogue image process. Digital image process is accomplishing variant laptop operations on digital image for varied functions like enhancing image quality, filtering pictures from noise. A digital image could be an illustration of 2 dimensional pictures as a finite set of digital values known as image components or pixels. Therefore, process a digital image by employing a digital computing is termed digital image processing. Creating a watermark, for your digital pictures, could be a good way to discourage individuals from repeating photos that you just could wear an Internet site. Whereas still permitting the image to be seen, most of the people can in all probability not need the image because it is with the watermark on that. Making a watermark and putting it on photos that you just attempt to post on the online can establish them as your own work and discourage individuals from repeating them or claiming them as their own. Here's an easy watermarked exposure. Their area unit many advantages to watermarking photos, including:

- Discourage thieves. It makes it terribly troublesome for someone to require credit for your work once your name is plastered across a photograph, hopefully discouraging him or her from even trying to do.
- Copyright. Though you don't would like a watermark on your image for it to be proprietary, doing though can give information those who the exposure relates to.
- Sense of satisfaction. It's very easy to share, copy, and save something that's printed on the net. As well, photo sharing websites area unit as common as ever. If you propose to post your photos on the net, having a watermark on that can offer you a way of satisfaction once you see your exposure printed for the planet to envision, stigmatization your name.

1.2. Watermarking Techniques

A digital watermark could be a reasonably marker covertly embedded associate degree exceedingly in a very noisetolerant signal akin to an audio, video or image knowledge. It's usually accustomed establish possession of the copyright of such signal. "Watermarking" is that the method of concealment digital data in a very carrier signal; the hidden data ought to, however doesn't have to, contain a relevance the carrier signal. Digital watermarks could also be accustomed verify the credibility or integrity of the signal or to inform the identification of its owners. It's conspicuously used for tracing copyright infringements and for government note authentication.

1.2.1. LSB

Least significant Bit (LSB): The LSB is that the simplest special domain watermarking technique to integrate a watermark in least vital bits of some haphazardly hand-picked pixels of the quilt image.

1.2.2 Spatial Embedding

The spatial domain represents the image within the style of pixels. The special domain watermarking embeds the watermark by modifying the intensity and also the color worth of some handpicked pixels. The strength of the special domain watermarking isSimplicity. Terribly low procedure complexness.

1.2.3 Transform or Frequency Embedding

The rework domain watermarking is achieving considerably success as compared to the spatial domain watermarking. Within the rework domain watermarking, the image is depicted within the kind of frequency. Within the rework domain watermarking methods, first image is regenerate by a predefined transformation. Then the watermark is embedded within the rework image or within the transformation coefficients. Finally, the inverse rework is performed to get the watermarked image. Most ordinarily used rework domain strategies is separate trigonometric function rework (DCT), separate moving ridge rework (DWT) and separate Fourier rework (DFT).

1.2.4 Secret encryption

Information concealment techniques square measure broadly speaking classified into four classes corresponding to, Covert channels, Steganography, obscurity and Copyright marking. The Steganography procedures are often linguistic or technical whereas the copyright marking procedures are often strong or fragile. Watermarking may be a kind of strong copyright marking technique, which may more be classified as perceptible or imperceptible watermarking. An entire classification of assorted knowledge concealment techniques.

In this kind of knowledge concealment, each the receiver and transmitter have common arranged secret keys. The key message is embedded into and extracted out of the stego image exploitation these keys. The keys are often singly shared between each parties exploitation some confidential channel before the particular transmission starts. The strength of this technique is its higher security. Parties nonetheless the supposed receiver cannot retrieve the key message or would force terribly high procedure time and power to retrieve it applying some brute force strategies, just in case they believe the presence of the key data. The hardiness of this technique, of course, lies with the secrecy of the keys and therefore the tough half during this technique is the way to share the keys between the sending and receiving parties maintaining their secrecies.

2. RELATED WORK

Digital watermarking is employed as a viable resolution to the requirement of copyright protection and authentication of multimedia system information in a very networked setting, since it makes potential to spot the author; owner; distributor or licensed client of a document. a replacement watermarking technique is conferred to feature a code to digital images: the strategy operates within the frequency domain embedding a pseudo-random sequence of real numbers in a very handpicked set of DCT coefficients. The embedded sequence is extracted while not resorting to the first image, in order that the projected technique represents a serious improvement to ways hoping on the comparison between the watermarked and original pictures. Experimental results demonstrate that the watermark is strong to most of the signal process techniques and geometric distortions. Watermarking could be a potential technique for copyright protection and multimedia system information authentication within the net. The watermarking method is thought of as a communication task. Code division multiple access (CDMA) modulation is employed to attain a superior performance in terms of lustiness and physical property. Each3-watermark bits area unit modulated into a 5bit MCDMA code. Then the MCDMA code is hid within the coefficients of a DCT block. To demonstrate the potency, simulations beneath varied conditions area unit conducted .The empirical results show that it will rise up against commonest attacks together with JPEG compression, rotating, resizing, cropping, noising and blurring etc. [3] A watermarking technique for embedding a big quantity of knowledge in digital still pictures whereas retentive a high sensory activity quality. The theme employs electronic communication techniques to attain high lustiness to straightforward image process operations. Data is embedded within the frequency domain by modulating handpicked DFT values of the image and mistreatment sets of orthogonal codes in a very fashion almost like CDMA. DFT values area unit sorted into completely different bands process freelance channels for carrying information. Blind recovery of the embedded information is achieved by analyzing the DFT values of the watermarked image. Computer simulations evaluate the performance of this scheme. [4] A digital watermark embeds Associate in an unbearable signal into information like audio, video and pictures, for a range of captioning functions, together with and copyright management. As watermarking is progressively used for a good kind of applications, varied properties of watermarks, like however they answer common signal transformations or deliberate attack, became vital concerns.

[5] A way supported CDMA and construction secret writing is employed so as to attain a high capabilitywatermarking theme. The bits of watermark area unit sorted along and for every sequence a distinct modulation constant is employed. Mistreatment the ripple remodel domain for embedding watermarks offers several blessings together with lustiness against intentional and unintentional attacks. It leads to low process demands whereas maintains identical high accuracy achieved by different.

3. EXPERIMENTAL DESIGN

3.1. Data Acquisition Phase

There are three approaches to obtain pictures automatically:

- The video input object, for use with an upheld equipment
- The gige cam object, for use with GigE Vision equipment as it were
- The Matrix cam object, for use with Matrix equipment as it were

The segment Acquisition Using Any Hardware relates to picture procurement utilizing the video input object with upheld equipment. In the event that you have GigE Vision or Matrix equipment, you can utilize the new interfaces for GigE Vision and Matrix, which give new questions, gigecam and Matrixcam. Alternately you can keep on using the current GigE Vision and Matrix connectors (gige and Matrix) with the videoinput object. You can likewise obtain pictures from upheld equipment utilizing the Image Acquisition Tool, a full UI that empowers you to set procurement properties, review the picture, and get pictures. For more data, see Acquisition Using the Image Acquisition Tool.

3.1.1. Spread Data Acquisition

A steganography method that utilizations picture as the spread media is called a picture steganography. Concealing mystery messages in computerized pictures is the most generally utilized technique as it can exploit the constrained force of the human visual framework (HVS) furthermore on the grounds that pictures have a lot of excess data that can be utilized to shroud a mystery message.

3.1.2. Mystery Data Acquisition

A steganography system that utilizations content as the spread media is known as a content steganography. It is a standout amongst the most troublesome sorts of the steganography method. This is on account of content documents have a little measure of repetitive information to shroud a mystery message

3.2. Pixel Matching Phase:

Utilizing BAT streamlining for pixel choice in the spread picture to insert the mystery picture.

3.2.1. BAT Optimization Method

The bat calculation is another swarm knowledge advancement strategy, in which the inquiry calculation is propelled by social conduct of bats and the wonder of echolocation to sense separation. In BA, every bat is characterized by its position x_i^{t} , speed v_i^{t} , recurrence fi, clamor A_i^{t} and the emanation beat rate r_i^{t} in a d-dimensional hunt space. The new arrangements x_i^{t} and speeds v_i^{t} at time step t are given by

$$f_i = f_{min} + (f_{max} - f_{min})\beta$$
$$v_i^t = v_i^{t-1} + (X_i^t - X_*)f_i$$
$$X_i^t = X_i^{t-1} + v_i^t$$

Where $\beta \in [0, 1]$ may be a random vector drawn from an even distribution. Here x* is that the current international best location (solution) that is found when comparing all the solutions among all the n bats.

For the native search half, once an answer is chosen among this best solutions, a replacement resolution for every bat is generated regionally exploitation stochastic process

$$X_{new} = X_{old} + \varepsilon A^t$$

where $\varepsilon \in [-1, 1]$ could be a scaling issue that could be a random variety, whereas $A_{t} = \< A_i^t \& gt$; is that the average loudness of all the kooky at time step t.

Furthermore, the loudness Ai and therefore the rate Rhode Island of pulse emission update consequently because the iterations proceed show.

$$A_i^{t+1} = \alpha A_i^t, r_i^{t+1} = r_i^0 [1 - \exp[(-\gamma t)]]$$

3.2.2. Least Significant Bit Embedding

The LSB is that the simplest spatial domain watermarking technique to engraft a watermark within the least significant bits of some arbitrarily chosen pixels of the duvet image. Example of least important bit watermarking:

Image: 10010101 00111011 11001101 01010101....

Watermark: 1 0 1 0....

Watermarked Image: 10010101 00111010 11001101 01010100...

The steps wont to engraft the watermark within the original image by exploitation the LSB: 1) Convert RGB image to gray scale image. 2) Create double exactitude for image. 3) Shift {most important most vital most important} bits to low significant bits of watermark image. 4) create least important bits of host image zero. 5) Add shifted version (step 3) of watermarked image to changed (step 4) host image. the most advantage of this technique is that it's simply performed on pictures. And it provides high sensory activity transparency. after we engraft the watermark by exploitation LSB the standard of the image won't degrade. the most downside of LSB technique is its poor strength to common signal process operations as a result of by exploitation this system watermark will simply be destroyed by any signal process attacks. it's not prone to attacks and noise however it's a great deal invisible.

3.2.3. Returning the Object:

Return the stego object with the enveloped data after the successful embedding. The stego object has been hidden while returning the object.

3.3 Algorithm For Fitness Function

$$fi - fn = \sum_{i=1}^{i=1} |Img(r_i, c_i) - D_i|$$

- Where I denotes the number of data characteristics to be hide.
- Img (_{ri,ci}) denotes the predicted image location for ith frequency
- D_i is the ith ASCII value for data to be hide.

3.4 Algorithm for BAT Optimization

$$for i = 1 to freq.$$

$$F_{Pi} = Rand[i]$$

$$FF_{Pi} = fit - fun[F_{Pi}]$$

$$end for$$

$$for j = 1 to G$$

$$for i = 1 to freq.$$

$$F_{Ci} = F_{Pi} + v_i$$

$$FF_{Ci} = fit - fun[F_{Ci}]$$

$$end for$$

$$for i = 1 to freq.$$

$$if (FF_{Ci} < FF_{Pi})$$

$$F_{Pi} = F_{Ci}$$

$$FF_{Pi} = FF_{Ci}$$

$$end if$$

$$end for$$

$$g_{best} = [FF_{Pi}]_{min}$$

$$end for$$

- Where F_{Pi} is the ith present frequency
- freq is the variable defined by user in BAT Optimization
- FF_{Pi} is the fitness value predicted by the fn. fit fun
- G are the number of iterations taken by the user
- F_{Ci} denotes ith child frequency
- V_i is the velocity for ith frequency

• *FF_{Ci}* stores the value generated by the fitness function for ith child frequency

4. RESULT ANALYSIS

4.1. Performance Evaluation Scenario

Security and authentication of information are important problems to be thought-about. Tons of analysis goes on to extend security and authentication. During this thesis we tend to square measure giving a brand new image watermarking methodology. This methodology will increase the safety and authentication by embedding multiple watermarks within the image while not reducing the standard of the image. Once learning literature accessible, variety of following issues still exist within the watermarking. Results Shows that performance of projected system is additional economical than previous ways. Whereas playing completely different attacks upon projected system the square error result's perpetually lesser than previous ways.

4.3. Results and Discussion

 Table 1: Squared Error results while performing attacks

					SB	Pr
		Meth	Metho	metho	Μ	ор
Мо		od in	d	d in	ß=0.	ose
del	Attacks	[32]	in[33]	[34]	2	d
1	Closed-loop	0.050	0	0.074	0	0
	Median				0.01	0.0
2	Filtering	0.091	0	0.118	6	02
					0.11	0.0
3	JPEG 10%	0.212	0.490	0.245	2	02
						0.0
4	JPEG 30%	0.061	0.485	0.199	0	02
	Gaussian				0.00	0.0
5	noise	0.071	0.473	0.146	1	01
	Salt & pepper					
6	noise	0.050	0	0.074	0	0
					0.00	0.0
7	Rotation 10	0.075	0.267	0.228	3	02
					0.00	0.0
8	Rotation 25	0.083	0.307	0.230	5	02
					0.00	0.0
9	Scaling 80%	0.073	0.283	0.234	7	02
10	Scaling 120%	0.060	0.240	0.204	0	0
					0.00	0.0
11	Shearing 10%	0.064	0.039	0.206	4	02
	Cropping				0.00	
12	10%	0.060	0	0.053	4	0
	Cropping				0.00	
13	20%	0.138	0	0.073	4	0
	Cropping				0.00	
14	30%	0.142	0	0.076	6	0
	Global	0.07/	0.054	0.405	0.00	0.0
15	bending	0.071	0.056	0.197	1	01
		0.055		0.005	0.00	0.0
16	HF bending	0.050	0	0.083	4	02
1.7	T . 1 1	0.055	0	0.074	0.00	
17	Jittering 1%	0.053	0	0.076	4	0

Above table shows the results of squared error while performing the 17 attacks on different methods. Result proves that proposed system has been more accurate than existing methods of digital image security. Below is the graphical representation of results given in table 1.



Chart1 : Squared Error results while performing attacks

Table 2: Mean of Squared Error results while performing attacks

Method in	Method in	method in	SBM	
[32]	[33]	[34]	ß=0.2	Proposed
0.083	0.155	0.148	0.010	0.001

Above Table shows the mean value of squared error of each method. Below is the graphical representation of table2 results.



Chart 2: Mean Squared Error results while performing attacks

5. CONCLUSION

Watermarking is AN emerging analysis space for copyright protection and authentication of the transmission. Most of the analysis goes on during this field; the rationale could be that there are such a large amount of pictures out there at web with none value, that has to be protected. In future, work could also be extended on totally different media like video, audio etc. by victimization this approach. Right away the planned approach is functioning solely with the photographs. During this treatise watermarks are embedded with the assistance of DWT- DCT-Viterbi. So, any work will be done to seek out another watermark embedding theme to extend the safety of Watermarked information.

REFERENCES

- [1]Y. Xiang, I. Natgunanathan, D. Peng, W. Zhou, and S. Yu, "A dual- channel time-spread echo method for audio watermarking," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 383–392, Apr. 2012.
- [2] Y. Xiang, D. Peng, I. Natgunanathan, and W. Zhou, "Effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time-spread echo-based audio watermark- ing," *IEEE Trans. Multimedia*, vol. 13, no. 1, pp. 2–13, Feb. 2011.
- [3] N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image water- marking in the ridgelet domain using universally optimum decoder," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 3, pp. 396–406, Mar. 2010.
- [4] E. Nezhadarya, Z. J. Wang, and R. K. Ward, "Robust image water- marking based on multiscale gradient direction quantization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1200–1213, Dec. 2011.
- [5] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compresseddomain video watermarking resistance to geometric distortions," *IEEE MultiMedia*, vol. 19, no. 1, pp. 70–79, Jan. 2012.
- [6] M. Lee, K.-S. Kim, and H.-K. Lee, "Digital cinema watermarking for estimating the position of the pirate," *IEEE Trans. Multimedia*, vol. 12, no. 7, pp. 605–621, Nov. 2010.
- [7] N. F. Johnson, Z. Duric, and S. Jajodia, "Recovery of watermarks from distorted images," in *Proc. 3rd Int. Workshop Inf. Hiding*, 1999, pp. 318–332.
- [8] F. Davoine, "Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares," in *Proc. EURASIP Signal Process. Conf.*, 2000, pp. 493–496.
- [9] P. Dong, J. G. Brankov, N. Galatsanos, and Y. Yang, "Geometric robust watermarking based on a new mesh model correction approach," in *Proc. IEEE Int. Conf. Image Process.*, Jun. 2002, pp. 493–496.
- [10] H. Zhang *et al.*, "Affine Legendre moment invariants for image water- marking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 20, no. 8, pp. 2189–2199, Aug. 2011.
- [11] J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk, "Exhaus- tive geometrical search and the false positive watermark detection probability," *Proc. SPIE, Secur. Watermarking Multimedia Contents V*, vol. 5020, pp. 203–214, Jun. 2003.
- [12] M. Barni, "Effectiveness of exhaustive search and template match- ing against watermark desynchronization," *IEEE Signal Process. Lett.*, vol. 12, no. 2, pp. 158–161, Feb. 2005.
- [13] J. J. K. Ó. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 303–317, May 1998.
- [14] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking

for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767–782, May 2001.

- [15] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG com- pression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, Aug. 2003.
- [16] X. Kang, J. Huang, and W. Zeng, "Efficient general printscanning resilient data hiding based on uniform log-polar mapping," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 1–12, Mar. 2010.
- [17] D. Rosiyadi, S.-J. Horng, P. Fan, X. Wang, M. K. Khan, and Y. Pan, "Copyright protection for e-government document images," *IEEE MultiMedia*, vol. 19, no. 3, pp. 62–73, Jul./Sep. 2013.
- [18] S. Pereira, J. J. K. Ó. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps," in *Proc. IEEE Int. Conf. Multimedia Comput. Syst.*, Jul. 1999, pp. 870–874.
- [19] S. Pereira and T. Pun, "Robust template matching for affine resis- tant image watermarks," *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123–1129, Jun. 2000.
- [20] S. Pereira and T. Pun, "An iterative template matching algorithm using the Chirp-Z transform for digital image watermarking," *Pattern Recognit.*, vol. 33, no. 1, pp. 173–175, Jan. 2000.
- [21] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," *IEEE MultiMedia*, vol. 12, no. 3, pp. 68–78, Sep. 2005.
- [22] M. Álvarez-Rodr iguez and F. Pérez-González, "Analysis of pilot-based synchronization algorithms for watermarking of still images," *Signal Process., Image Commun.*, vol. 17, no. 8, pp. 611–633, Sep. 2002.
- [23] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Trans. Image Process.*, vol. 13, no.
 2, pp. 145 –153, Feb. 2004.
- [24] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Dig- ital watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2140–2150, Dec. 2005.
- [25] J. S. Seo and C. D. Yoo, "Image watermarking based on invariant regions of scale-space representation," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1537–1549, Apr. 2006.
- [26] J.-S. Tsai, W.-B. Huang, C.-L. Chen, and Y.-H. Kuo, "A featurebased digital image watermarking for copyright protection and content authentication," in *Proc. IEEE Int. Conf. Image Process.*, Sep./Oct. 2007, pp. V-469–V-472.
- [27] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 40, no. 3, pp. 278–286, May 2010.
- [28] Y.-T. Lin, C.-Y. Huang, and G. C. Lee, "Rotation, scaling, and translation resilient watermarking for images," *IET Image Process.*, vol. 5, no. 4, pp. 328–340, Jun. 2011.
- [29] J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of opti- mal feature region set for robust digital image watermarking," *IEEE Trans. Image Process.*, vol. 20, no. 3, pp. 735–743, Mar. 2011.
- [30] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Int. Workshop Inf. Hiding*, 1998, pp. 218–238.

- [31] J. Dugelay, S. Roche, C. Rey, and G. Doerr, "Still-image watermarking robust to local geometric distortions," *IEEE Trans. Image Process.*, vol. 15, no. 9, pp. 2831–2842, Sep. 2006.
- [32] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777–790, Jun. 2008.
- [33] L. Xin-Wei, G. Bao-Long, L. Lei-Da, and S. Hong-Xin, "A new histogram based image watermarking scheme resisting geometric attacks," in *Proc. 5th Int. Conf. Inf. Assurance Secur.*, Aug. 2009, pp. 239–242.
- [34] C. Deng, X. Gao, X. Li, and D. Tao, "Local histogram based geo- metric invariant image watermarking," *Signal Process.*, vol. 90, no. 12, pp. 3256–3264, Dec. 2010.
- [35] S.-W. Jung, L. T. Ha, and S.-J. Ko, "A new histogram modification based reversible data hiding algorithm considering the human visual system," *IEEE Signal Process. Lett.*, vol. 18, no. 2, pp. 95–98, Feb. 2011.
- [36] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 111–120, Jan. 2013.
- [37] C.-S. Lu, S.-W. Sun, C. Y. Hsu, and P.-C. Chang, "Media hashdependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection," *IEEE Trans. Multimedia*, vol. 8, no. 4, pp. 668–685, Aug. 2006.
- [38] P. Thévenaz, T. Blu, and M. Unser, "Image interpolation and resam- pling," in *Handbook of Medical Imaging, Processing and Analysis*, N. B. Isaac and I. N. Bankman, Eds., 2nd ed. Burlington, VT, USA: Academic, 2009, ch. 28, pp. 465–493.
- [39] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20– 46, Sep. 2000.
- [40] P. Zhu and P. Chirlian, "On critical point detection of digital shapes," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 17, no. 8, pp. 737–748, Aug. 1995.
- [41] S. Li, J. J. Ahmad, D. Saupe, and C.-C. J. Kuo, "An improved DC recovery method from AC coefficients of DCT-transformed images," in *Proc. 17th IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2085–2088.
- [42] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600– 612, Apr. 2004.
- [43] C. A. Glasbey and K. V. Mardia, "A review of image-warping methods," J. Appl. Statist., vol. 25, no. 2, pp. 155–171, 1998.
- [44] D. Delannay, J.-F. Delaigle, B. M. M. Macq, and M. Barlaud, "Compensation of geometrical deformations for watermark extraction in digital cinema application," *Proc. SPIE, Secur. Watermarking Multimedia Contents III*, vol. 4314, pp. 149–157, Jan. 2001.
- [45] V. Licks, F. Ourique, R. Jordan, and F. Perez-Gonzalez, "The effect of the random jitter attack on the bit error rate performance of spatial domain image watermarking," in *Proc. Int. Conf. Image Process.*, Sep. 2003, pp. II-455–II-458.