ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Robust and Secure Image Watermarking using DWT-SVD and Chaotic Map

Sanpreet Singh[1], Savina Bansal[2], Sukhjinder Singh[3]

Research Scholar, Department of Electronics & Communication Engineering,
Giani Zail Singh Campus College of Engineering & Technology, Bathinda, India[1]

Professor, Department of Electronics & Communication Engineering,
Giani Zail Singh Campus College of Engineering & Technology, Bathinda, India[2]

Assistant Professor, Department of Electronics & Communication Engineering,
Giani Zail Singh Campus College of Engineering & Technology, Bathinda, India[3]

Abstract*:* Various digital image watermarking techniques have been proposed by researchers from time to time. In this paper, a noval image watermarking is proposed (DSAWM) based on DWT-SVD and chaos based encryption using Arnold cat map. The DWT-SVD approach is used to increase the robustness while encryption helps in making the watermark more secure. From the simulation results, it can be concluded that DSAWM algorithm gives better result for rotation, noise and JPEG compression attacks as compared with other relevant work.

Keywords: Robust, Watermarking, Discrete Wavelet Transform, Singular Value Decomposition and Arnold Cat Map.

I. INTRODUCTION

With the development of digital technology, computer science, communication and network, online services are widely launched but it's illegal copying, piracy, malicious manipulations and counterfeiting has triggered the need for multimedia protection [1]. Digital watermarking is an effective way to solve these problems as it provides copyright protection of data by embedding additional information (digital signature or watermark) such that it can be detected, extracted later to make an assertion about the multimedia data. In literature, the host file is called the asset and the bit stream is called the message. Stegnography and cryptography are other well known methods. Digital watermarking [2] has many applications such as broadcasting monitoring, owner identification, content authentication and file reconstruction. A good watermarking scheme should aim at keeping the watermark robust against malicious attacks in spatial, spectral and hybrid domain. It should find a good balance between robustness and imperceptibility. Digital image watermarking techniques always works in two domains either spatial or transform domain. In spatial domain, the embedding as well as extraction of watermark is done by modifying the intensity and the colour value of some selected pixels. Various spatial domain algorithms are - Least Significant bit (LSB), patchwork method with streak block mapped coding, method based on district intersecting. Various transform domain algorithms are spread spectrum, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). To ensure security of watermark, it is encrypted before embedding. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Keys can be public or private. Public keys are those which are made available to all via a public accessible directory while private keys are those which remain confidential to its respective owners. Public – Private key is very effective pair as whatever is encrypted using public key is decrypted by a private key. Every digital watermarking technique includes two algorithms: one as the embedding algorithm and other as the detecting algorithm as depicted in the Fig. 1(a) and 1(b) respectively. This paper proposes an algorithm of digital image watermarking using Discrete Wavelet Transform and Singular Value Decomposition and chaos based encryption. DWT-SVD technique is used to embed watermark. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. Chaotic output signals, presents random statistical properties, which are used for both confusion and diffusion operations in a cryptosystem. Random statistical property makes watermark random in attackers eye, but is decrypted by authorized person. The host image is decomposed using one level DWT-SVD, watermark is encrypted using chaotic map and decomposed using one level DWT-SVD. Encrypted watermark’s lower frequency singular value is embedded in host image lower frequency singular value. Inverse Discrete Wavelet transform (IDWT) of watermarked image is done to reconstruct it. Watermark is extracted and decrypted. Remaining paper has been organized as follows: Section 2 deals with Related Work, Section 3 with Proposed Algorithm, Section 4 with Experimental Results and Simulations, Section 5 with Conclusion.

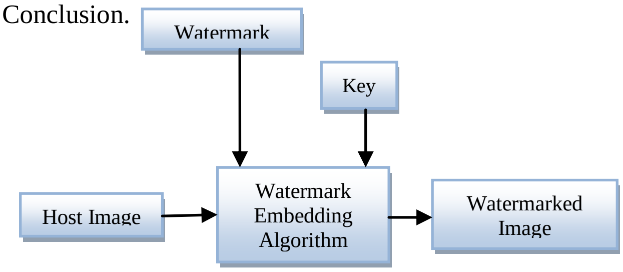


Fig. 1(a). Watermark Embedding

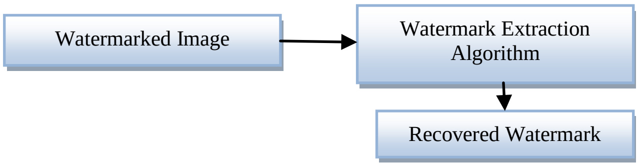


Fig. 1(b). Watermark Extraction

A. Discrete Wavelet Transform

Wavelet Transforms (WT) and Fourier Transforms (FT) converts spatial domain information to frequency domain. The fourier transformed signal X(f) gives the global frequency distribution of the time signal x(t). The original signal can be reconstructed using the inverse fourier transform. Equation (1) and (2) represents fourier and inverse fourier transform of time signal x(t).

$$\mathrm{X}(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}\mathrm{d}\,t .... (1)$$

$$\mathrm{x}(t)=\int_{-\infty}^{\infty} X(f)e^{j2\pi ft}\mathrm{d}\,f ....(2)$$

The advantage of wavelet over the fourier is local analysis. Wavelet analysis can reveal signal aspects like discontinuities, breakdown points etc. more clearly than FT. A wavelet basis set starts with two basis functions: father wavelet $\varphi(t)$ and mother wavelet $\psi(t)$, by scaling and transformation of these orthogonal functions complete basis set is obtained [3]. Wavelet transform can be expressed by equation 3 as

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\psi^{*}{}_{(a,b)}(x)dx \quad ....(3)$$

A filter bank separates the signal into various frequency bands. The coefficients produced by the low-pass filter are called coarse coefficients. The coefficients produced by the high-pass filter are called fine coefficients. Coarse coefficients provide information about low frequencies, whereas fine coefficients provide information about high frequencies. An original image can be decomposed into LL, HL, LH and HH bands where LL is lower frequency, HL is horizontal, LH is vertical and HH is diagonal band respectively. The low-frequency sub-band can further be decomposed into LL1, HL1, LH1 and HH1. By doing this the original image can be decomposed for n level wavelet transformations. A two-dimensional image after three-time DWT decomposition is shown in Fig. 2 where L represents low-pass filter, H represents high-pass filter [4].

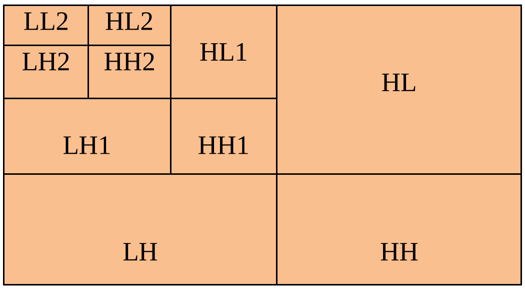


Fig. 2. Three Level Image Decomposition

Embedding the watermark in the lower frequency is more resistant to JPEG compression, wiener filtering, gaussian noise, scaling and cropping but lower frequency band is very sensitive area as it contains maximum information so any changes will be detected by human eye, while higher frequency sub-band is more resistant to histogram equalization, intensity adjustment and gamma correction and is less sensitive to human vision hence changes are not easily detectable but compression removes watermark in high frequency. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks [15].

B. Singular Value Decomposition (SVD)

An image can be represented as a matrix of positive scalar values. SVD for any image say A of size $m \times m$ is a factorization of the form given by A = USV, Where U and V are orthogonal matrices in which columns of U are left singular vectors and columns of V are right singular vectors of image A. S is a diagonal matrix of singular values in decreasing order. Advantage of embedding watermark in SVD are as below

1) A small agitation added in the image, does not cause large variation in its singular values.
2) The singular value represents intrinsic algebraic image properties.

C. Encryption

To increase security of watermark being embedded it is encrypted before embedding. Various Encryption Algorithms are Data Encryption Standards (DES), Advanced Encryption Standards (AES), RSA, Blowfish, Serpent, Confusion [5] and Diffusion and chaos based encryption.

II. RELATED WORK

Xueyi *et al.* [9] proposed an image watermarking algorithm based on zernike moment. This algorithm resists geometric attacks like rotation and scaling and hence makes watermark more robust.

Chittaranjan *et al.* [7] used cross chaos and arnold map to encrypt watermark before embedding it in host image. The behaviour of the chaos is unpredictable which makes attacker difficult to decrypt it. The possibility for self-synchronization of chaotic oscillations has sparked an avalanche of works on application of chaos in cryptography.

Henry-Ker *et al.* [18] proposed a private key encryption for two dimensional image data. Along with encryption, lossless compression is performed simultaneously. The testing results and analysis demonstrate the characteristics of the proposed scheme. This scheme can be applied for problems of data storage or transmission in a public network.

Chang-Mok et al. [16] proposed image encryption using binary phase XOR operation [8]. Since pixels of the image are highly correlated to its neighbouring pixels, hence there is need of any technique which can shuffle pixels so as to reduce the correlation among pixels so called transformation of image.

Tapas *et al.* [13] suggested digital watermarking techniques along with encryption of watermark using bitxor with random values. These two technologies are complimenting each other, and the increased security of the digital artifacts can be achieved by using benefits of the both. The experimental results demonstrate the high

DOI 10.17148/IJARCCE.2015.4926

robustness of the proposed algorithm to various image processing attacks like noise additions, rotations, cropping, filtering.

Tao *et al.* [6] proposed an algorithm on image watermarking using integer to integer wavelet transforms. Watermark is embedded in the significant wavelet coefficients [14] by a simple XOR operation. After the wavelet transform, the significant coefficients are selected and modified according to watermark. Simulation results suggests that watermark is robust to various operations such as JPEG compression, random and gaussian noise and mean filtering. Further the method avoids complicated computations and high computer memory requirement that are the main drawbacks of common frequency based watermarking algorithms.

Mingli *et al.* [12] proposed a novel robust image watermarking scheme based on discrete wavelet transform (DWT), singular value decomposition (SVD), and chaotic mixtures. In this method, the singular values of the encrypted watermark are embedded on the singular values of the inscribed circle domain of normalized cover image's DWT sub-bands. Experimental results illustrate that this approach is robust to a wide range of attacks, especially geometrical attacks.

Asia *et al.* [10] proposed selective image encryption using confusion and diffusion which distorts correlation among neighbouring pixels. Confusion is the process in which pixels of the image is substituted by randomly generated values. Confusion is carried out using arnold cat map [17]. Arnold cat map generates chaotic numbers which will accomplish encryption process. Diffusion is the process in which the pixels of image are shuffled within image. Henon and 2D Baker chaotic maps are used for diffusion.

Sunita *et al.* [11] proposed key based encryption algorithm called Byte Rotation Encryption Algorithm (BREA) with parallel encryption model which enhances security as well as encryption.

III. PROPOSED ALGORITHM (DSAWM)

In this Paper, an algorithm is proposed which makes watermark both robust and secure. DWT-SVD makes it robust, while encryption makes it secure. Following sections will deal with watermark encryption, embedding, extraction, decryption process and performance parameters.

A. *Encryption Technique*

This research paper uses arnold cat map for encryption. Arnold cat map is a chaotic map from the torus into itself. This transformation has determinant equal to unity. Number of iterations is defined as key and its periodicity is number of iterations after which transformed image gets converted back into original image. Shearing in X and Y direction, modulus of results after shearing process do scrambling.

Fig. 3 depicts encryption steps, while Fig.4 depicts encryption of watermark.

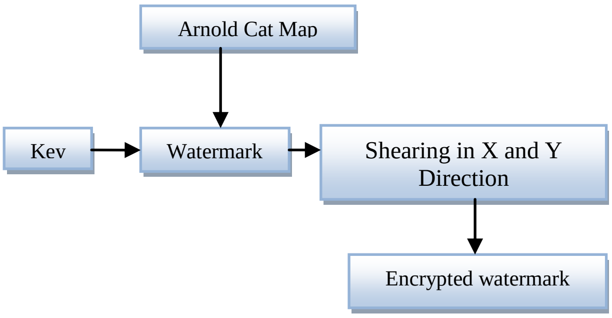


Fig. 3. Watermark Encryption using Arnold Map

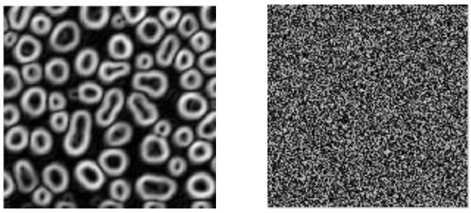


Fig. 4. Watermark and its Encryption

B. *Watermark Embedding Algorithm*

This section deals with watermark embedding process. DWT-SVD of both encrypted watermark (M*M) as well as host image (N*N) is done. Watermark's lower frequency singular value is inserted in host image lower frequency singular value. Inverse Discrete Wavelet Transform is used to reconstruct watermarked image.

Steps for Watermark Embedding

1 Use one level Haar DWT to decompose the host image into four sub bands (i.e. LL1, LH1, HL1 and HH1).

2 Apply SVD to LL1 sub band i.e., SVD to LL1 sub band, where A_h=LL1

$$A_h = U_h*S_h*V_h\text{..............................} (4)$$

3 Use Arnold cat map to encrypt watermark.

4 Use one level Haar DWT to decompose the watermark into four sub bands (i.e. LLW1, LHW1, HLW1 and HHW1).

5 Apply SVD to LLW1 sub band, where A_w = LLW1.

$$A_w = U_w*S_w*V_w\text{.............................}(5)$$

6 Modify the singular value of A_h by embedding singular value of W such that

$$S_{wm}= S_h+\alpha\times S_w\text{.............................}(6)$$

Where S_{wm} is the singular value of the watermarked image. α is the embedding coefficient.

7 Apply SVD to modified singular matrix S_{wm} i.e.,

$$S_{wm'}=U_h*S_{wm}*V_h^t\text{ ....}(7)$$

Wavelet Reconstruction is done using inverse discrete wavelet. Fig. 5 depicts watermark embedding algorithm.

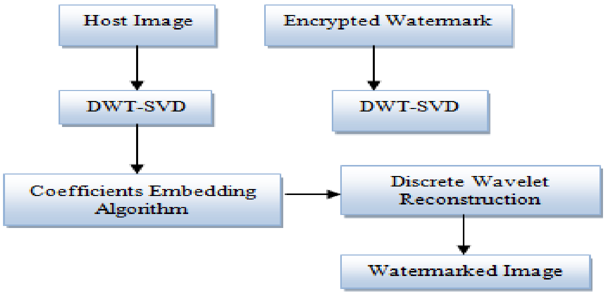

Host Image
Encrypted Watermark
DWT-SVD
DWT-SVD
Coefficients Embedding Algorithm
Discrete Wavelet Reconstruction
Watermarked Image

Fig. 5. Watermark Embedding algorithm

DOI 10.17148/IJARCCE.2015.4926

C. Watermark Extraction Algorithm

Extraction is non blind. Inverse arnold cat map decrypt it with a key. Private key is used which is confidential

Steps for Watermark Extraction

1 Apply One level Haar DWT to decompose the watermarked image $S_{wm'}$ in to four sub bands (i.e., WM_LL, WM_LH, WM_HL, *and* WM_HH).
2 Apply SVD to WM_LL sub band, where $A_{wm'}$ = WM_LL
$$A_{wm'}=U_e*S_e*V \text{ ……………………..(8)}$$
3 Extraction algorithm is as below
$$S_{extraction}=(S_e-S_h)/\alpha\text{…………….(9)}$$
4 Watermark is reconstructed using inverse discrete wavelet transform.
5 Inverse Arnold cat map decrypt it with a key.

Fig. 6 depicts watermark extraction algorithm.

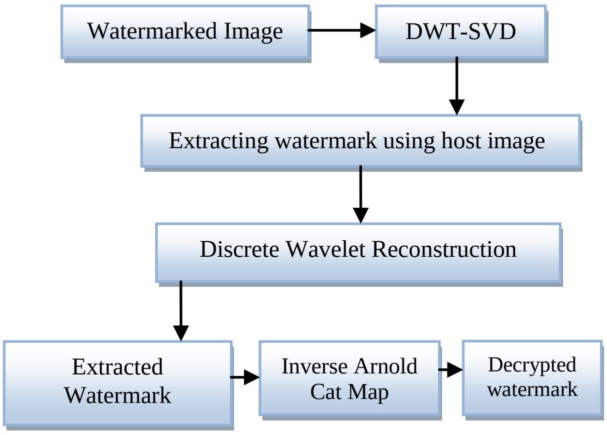


Fig. 6. Watermark Extraction Algorithm

D. Performance Parameters

To check the robustness of work, clarity and visibility of extracted watermark, performance parameters are calculated. Normalized cross correlation depicts robustness while peak signal to noise ratio tells about the visibility and clarity of extracted watermark and these are discussed in the section 1.1 and 1.2 respectively.

1.1 Normalized Cross Correlation

This research paper focuses on making the watermark robust. To achieve robustness, normalized cross correlation is calculated. If after the attacks, correlation among the pixels is least disturbed, it signifies robust watermark. Watermark is subjected to various attacks such as rotation, scaling, compression, contrast, noise and correlation among pixels of watermark and decrypted watermark is calculated, if it results in 1(100%) or nearly equal to 1, it reveals watermark is robust. As it goes on decreasing clarity of watermark goes on decreasing. Mathematically, Normalized Cross Correlation can be expressed by Equation 10

$$\gamma(\mathrm{u,v}) = \frac{\sum_{\mathrm{x,y}}[\mathrm{f(x,y)}-\bar{f}_{\mathrm{u,v}}][\mathrm{t(x-u,y-v)}-\bar{t}]}{\{\sum_{\mathrm{x,y}}[\mathrm{f(x,y)}-\bar{f}_{\mathrm{u,v}}]^2\sum_{\mathrm{x,y}}[\mathrm{t(x-u,y-v)}-\bar{t}]^2\}^{0.5}}\text{..........(10)}$$

Where, f = image
$\bar{t}$ = mean of the template
$\bar{f}_{u,v}$is the mean of f(x,y) in the region under template.

1.2 Peak Signal to Noise Ratio

It is measure of peak error. This ratio is a quality measurement between two images (original watermark and decrypted watermark in this paper). More value of PSNR indicates quality of watermark is preserved after undergoing attacks. For computing it, mean square error is calculated as

$$\text{MSE}=\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2\text{…..........(11)}$$

Where I_1 and I_2 are two images.

$$\text{PSNR} = 10\log_{10}(R^2|MSE)\text{……….........(12)}$$

Where R is maximum fluctuation in input image.

IV. EXPERIMENTAL RESULTS AND SIMULATIONS

In this thesis work, a digital image watermarking algorithm (DSAWM) had been implemented using MATLAB platform. Performance of the same had been analysed by calculating Normalized Correlation (NC), Peak Signal To Noise Ratio (PSNR), Mean Square Error (MSE) for various attacks such as cropping, scaling, contrast, rotation and compression. Moreover, the performance of DSAWM had been compared with Tapas *et al.* [13]. Fig. 7 depicts host and watermark image.

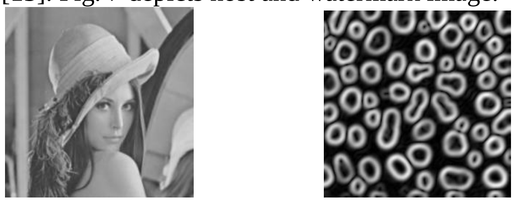
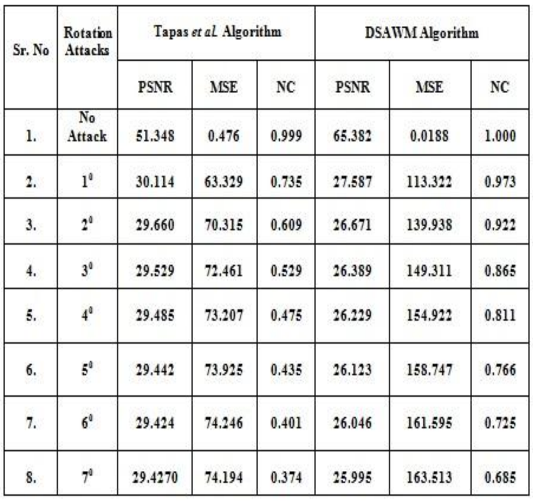


Fig. 7. Host and Watermark image

A Rotation Attacks

Watermarked image was subjected to rotation attacks i.e, image is rotated using different angles. Function imrotate is used to rotate the image, setting the pixels outside the rotated image equal to zero. Rotation using different angles will give different results. Table 1(a) shows performance analysis of rotation attack on both the algorithms.

Table 1(a): Performance comparison for rotation attack



Sr. No	Rotation Attacks	Tapas *et al.* Algorithm			DSAWM Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC
1.	No Attack	51.348	0.476	0.999	65.382	0.0188	1.000
2.	1^0	30.114	63.329	0.735	27.587	113.322	0.973
3.	2^0	29.660	70.315	0.609	26.671	139.938	0.922
4.	3^0	29.529	72.461	0.529	26.389	149.311	0.865
5.	4^0	29.485	73.207	0.475	26.229	154.922	0.811
6.	5^0	29.442	73.925	0.435	26.123	158.747	0.766
7.	6^0	29.424	74.246	0.401	26.046	161.595	0.725
8.	7^0	29.4270	74.194	0.374	25.995	163.513	0.685

Fig. 8(a) describes the 5^0 rotation effect on both the algorithms visually.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

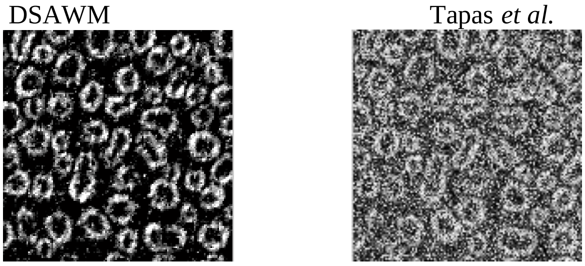


Fig. 8(a). Decrypted watermark after 5^0 rotation of watermarked image

As seen from the Table 1(a), the proposed algorithm is better able to survive the rotational attack. Form Fig. 8(a), it can be depicted that extracted watermark quality of DSAWM is much better visually as compared to Tapas *et al.*

B. Noise Attacks

Watermarked image was subjected to various noise attacks such as salt & pepper, gaussian, local var, poisson and speckle. Noise distorts the correlation among pixels, hence decreases visibility of image. Results in terms of performance parameters (PSNR, MSE, NC) are shown in Table 1(b).

Table 1(b): Performance comparison for noise attack

Sr. No	Noise Attack	Tapas *et al.* Algorithm			DSAWM Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC
1	Salt & Pepper Noise	29.632	70.766	0.560	27.879	105.956	0.860
2	Gaussian Noise	29.739	69.042	0.637	28.645	88.820	0.906
3	LocalVar	29.533	72.399	0.523	28.081	101.146	0.804
4	Poisson	31.073	50.783	0.829	31.322	47.955	0.985
5	Speckle	29.642	70.6020	0.5848	28.212	98.145	0.873

Fig. 8(b) describes the effect of localvar noise attack visually.

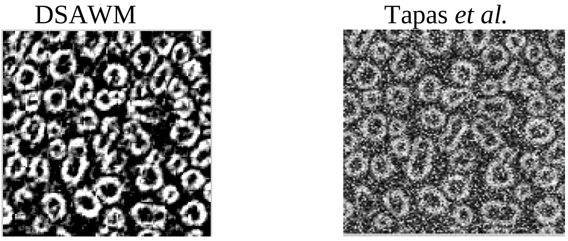


Fig. 8(b). LocalVar Attack

From the Table 1(b), It is gathered that DSAWM gives better result for the normalized cross correlation with respect to Tapas *et al*. whereas for the PSNR, results are comparable. From Fig. 8(b), it can be said that quality of DSAWM is better visually as compared to Tapas *et al.*

C. JPEG Compression

Compression reduces the size of the image. Compression can be lossy or lossless. Use of either lossy or lossless depend upon the application. RAW, PNG and BMP are lossless file formats whereas JPEG compression is lossy compression which reduces bits by identifying unimportant information and particularly used for digital photography. For web usage, where the amount of data used for an image is important, JPEG compression is very important. Watermarked was subjected to JPEG compression with different quality factor. Table 1(c) shows performance analysis of JPEG compression on both the algorithms.

Table 1(c): Performance comparison for JPEG compression attack

Sr. No	JPEG Compression with quality factor (Q)	Tapas *et al.* Algorithm			DSAWM Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC
1	No Attack	51.348	0.476	0.999	65.382	0.0188	1.000
2.	Q = 10	31.924	41.743	0.871	32.267	38.575	0.992
3.	Q = 20	32.907	33.289	0.905	36.089	16.001	0.996
4.	Q = 30	32.739	34.606	0.899	35.316	19.119	0.995
5.	Q = 40	33.342	30.120	0.916	36.932	13.177	0.997

Fig. 8(c) shows the effect of JPEG compression at quality factor = 10 on both the algorithms visually.

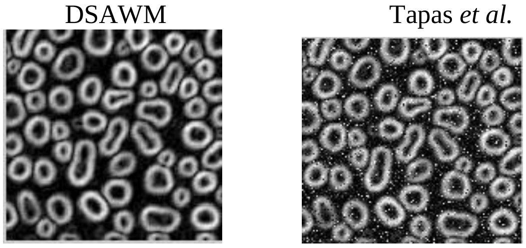


Fig. 8(c). JPEG compression attack with Q =10

From the Table 1(c), it can be concluded that both the algorithms shows good results with different quality factors hence both are more able to survive the JPEG compression attack.

D. Contrast attacks

Table 1(d): Performance comparison for contrast attack

Sr. No	Contrast Attack	Tapas *et al.* Algorithm			DSAWM Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC
1	No Attack	51.348	0.476	0.999	65.382	0.0188	1.000
2	Contrast ([0.3 0.7],[])	29.371	75.150	0.258	30.335	60.196	0.438
3.	Contrast ([0.1 0.9],[])	29.478	73.327	0.446	30.885	53.036	0.778
4.	Contrast ([0.2 0.7],[])	29.349	75.529	0.134	36.069	16.073	0.380
5.	Contrast ([0 1],[])	51.348	0.476	0.999	65.382	0.0188	1.000
6.	Contrast ([0.3 1],[])	29.217	77.865	0.021	24.671	221.806	0.183

DOI 10.17148/IJARCCE.2015.4926

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Contrast adjusts image intensity value. Watermarked image undergoes contrast attacks by setting different value of low_in, high_in, low_out and high_out. Values below low_in and high_out are clipped. Values lies between 0 and 1. Table 1(d) shows performance analysis of contrast attacks on both the algorithms.

Fig. 8(d) shows contrast effect of on both the algorithms with the help of images

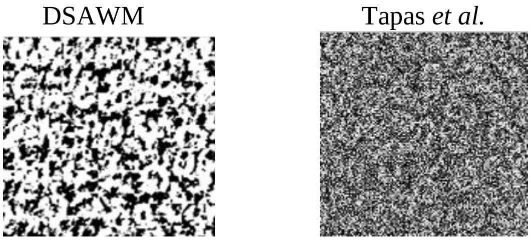


Fig. 8(d). Contrast Attack

As seen from the table 1(d), it can be gathered that both the algorithms fails to survive contrast attacks. From the Fig. 8(d), it can be seen that both the algorithms fails to survive attacks visually.

E. Scaling Attack

Watermarked image was subjected to different scaling effects. Scaling can be either scaling up or down. Table 1(e) shows performance analysis of scaling effect on both algorithms.

Table 1(e): Performance comparison for scaling attack

Sr. No	Scaling Attacks	Tapas *et al.* Algorithm			DSACM Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC
1	No Attack (256*256)	51.348	0.476	0.999	65.382	0.0188	1.000
2.	(256*254)	29.500	72.957	0.464	28.029	102.358	0.745
3.	(230*229)	29.244	77.378	0.0857	26.767	136.866	0.132
4.	(258 *250)	29.248	77.310	0.0918	27.507	115.422	0.109
5.	(257 *253)	29.361	75.328	0.305	27.723	109.841	0.512

Fig. 8(e) shows scaling effect on both the algorithms visually.

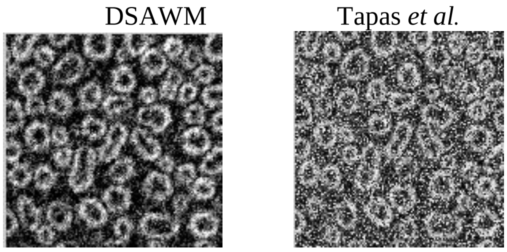


Fig. 8(e). Scaling Aattack

From the table 1(e), it can be depicted that algorithms shows poor performance when subjected to scaling attacks.

V. CONCLUSION

In this proposed algorithm (DSAWM), a new digital watermarking scheme is proposed in this work. The combined approach of DWT-SVD and chaos maps are exploited to make watermark more robust and secure. Performance has been analysed in terms of normalized cross correlation, peak signal to noise ratio and mean square error. To check the robustness of the proposed algorithm (DSAWM), it is compared with relevant work and from the simulation results, it is gathered that proposed algorithm is better able to survive rotation, noise and JPEG compression while it shows poor performance for scaling and contrast attacks but on the other hand time taken by DSAWM algorithm is about 60 seconds for total process, whereas Tapas *et al.* algorithm takes 20 seconds.

REFERENCES

[1] M. Chandra, S. Pandey and R. Chaudhary, *"Digital watermarking technique for protecting digital images"*, 3rd IEEE International Conference on Computer Science and Information Technology, vol. 7, pp. 226-233, 2010.

[2] C. Ingemer, M. Mathew, B. Jeffrey, F. Jessica and K. Ton, *Digital Watermarking and Stegnography*, 2nd Edition, Burlington, USA, Morgan Kaufmann Publishers, 2007.

[3] A. Graphs, *"An introduction to wavelets"*, IEEE Computing in Science and Engineering, vol. 2, issue 2, pp. 50-61, 2002, ISSN:1070-9924.

[4] J. Mei, S. Li and X. Tan, *"A Digital Watermarking Algorithm based on DCT And DWT"*, in proceedings of International Symposium on Web Information Systems and Applications, pp. 104-107, May 22-24, 2009, ISBN 978-952-5726-00-8.

[5] G. Sayed and M. Ajmal Bangash, *"Enhanced Block based Color Image Encryption Technique with Confusion"*, IEEE Transactions on International Multi-topic Conference, pp. 200-206, 2008.

[6] T. Chen and J. Wang, *"Image Watermarking Method using Integer-to-Integer Wavelet Transforms"*, Tsinghua Science and Technology, vol. 7, issue 5, pp.508-512, October 2002, ISSN:1007-0214.

[7] P. Chittaranjan, R. Shibani and B. Ajay kumar, *"Non Blind Digital Watermarking Technique using DWT and Cross Chaos"*, 2nd International Conference on Communication, Computing and Security Procedia Technology, vol. 6, pp. 897-904, 2012.

[8] P. Rinki and T. Vijay Kumar, *"Image Encryption using Random Scrambling and XOR Operation"*, International Journal of Engineering Research & Technology, vol.2, issue 3, pp. 1-7, 2013, ISSN: 2278-0181.

[9] X. Ye, M. Deng, Y. Wang and J. Zhang, *"A Robust DWT-SVD Blind Watermarking Algorithm based on Zernike Moments"*, International Conference on Communication Security, pp. 1-6, May 2014.

[10] M. Asia and A. Naser, *"Selective Image Encryption with Diffusion and Confusion Mechanism"*, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, issue 7, pp. 5-12, 2014, ISSN: 2277128X.

[11] B. Sunita, B. Anita and S. K. Sharma, *"A New Approach towards Encryption Schemes: Byte –Rotation Encryption Algorithm"*, in proceedings of the World Congress on Engineering and Computer Science, vol. 2, October 24-26, 2012, ISBN: 978-988-19252-4-4

[12] Z. Mingli, Z. Qiang and Z. Changjun, *"Robust Digital Image Watermarking in DWT-SVD Domain"*, Artificial Intelligence and Computational Intelligence, Lecture Notes in Computer science, vol. 7003, pp. 75-84, 2011.

[13] B. Tapas, B. B and C. BN, *"Image Security through DWT & SVD based Watermarking and masking with Encryption"*, International Journal of Recent Development in Engineering and Technology, vol.1, issue 1, pp. 6-11, 2013, ISSN: 2347-6435.

[14] X. Xiang-Gen, B. Charles and A. Gonzalo, *"Wavelet Transform Based Watermark for Digital Images"*, Optical Express 497, vol. 3, issue 12, 1998.

[15] E. Ganic and A. M. Eskicioglu, *"Robust DWT-SVD domain image watermarking : Embedding data in all frequencies"*, in proceedings of Workshop on Multimedia Security, pp. 166-174, Magdeburg, Germany, 2004.

[16] S. Chang-Mok, S. Dong-Hoan, C. Kyu-Bo, L. Ha-Woo and K. Soo-Joong, *"Multi-Level Image Encryption by Binary Phase XOR Operations"*, The 5th Pacific Rim Conference on Lasers and Electro-Optics, CLEO/Pacific Rim 2003, Taipei 106, Taiwan, 15 -19 Dec. 2003.

[17] S. Lenka and Z. Ivan , *"Arnold Cat Map and Sinai as Chaotic Numbers Generators in Evolutionary Algorithms"*, AETA 2013: Recent Advances in Electrical Engineering and Related Sciences, vol. 282, pp. 381-389, Berlin, Heidelberg, Springer, 2014.

[18] C. Henry-Ker and L. Jiang-Long, *"A linear quadtree compression scheme for image encryption"*, Signal Processing: Image Communication, vol. 10, issue 4, pp. 279-290, September 1997.

DOI 10.17148/IJARCCE.2015.4926