Asian Journal of Information Technology 15 (19): 3858-3869, 2016
ISSN: 1682-3915

Copyright Protection of Dual Color Images Based on Singular Value Decomposition Using Improved Arnold

[1]A. Lakshmi Priya and [2]S. Letitia
[1]Department of ECE, Global Institute of Engineering and Technology,
Vellore, Tamil Nadu, India
[2]Department of ECE, Thanthai Periyar Government Institute of Engineering and Technology,
Vellore, Tamil Nadu, India

Abstract: The main intention of a majority of the researches is paying attention to digital image watermarking technology is to improve the robustness to attacks. In this paper a new dual watermarking technique using singular value decomposition and improved Arnold transform is used to balance the trade-off between imperceptibility and robustness of the watermarks. In the proposed technique the secondary watermark is scrambled using improved Arnold and embedded into primary watermark the resultant new image is used as watermark for the Host image. The insertion and extraction of the watermarks are performed using the discrete wavelet transform, discrete cosine transform and singular value decomposition. This algorithm enhances the visual imperceivability of the watermarked image and robustness against various removals and geometric attacks. Numerous experiments have been performed; the numerical analysis demonstrates the improvement in embedding capacity, visual imperceptibility and watermark robustness compared with subsisting methods.

Key words: Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), Peak Signal to Noise Ratio (PSNR) and Normalized correlation (NC)

INTRODUCTION

Illegal copying, meddling, editing and copyright protection have become a very substantive issue in the multimedia industry. The exceptional increase in the generation, transmission and prompt use of the cyberspace in many applications is the solitary case of that. This has bestowed to a reversion of an advancing majority of the researches in this neighborhood to get a technical barrier to protect the multimedia capacity (Jia, 2014). To dissolve these issuances, Digital watermarking technology has swept up the attention of the researchers to furnish a standard resolution. Likened with grayscale images, color image watermarking has become more salient features because it has more cracking capability and fidelity. That is a greater measure of data can be hidden in color image and can achieve higher fidelity because the color perception doesn't only depend on the luminance but also on the chrominance (Subramanyan *et al*., 2011; Potdar *et al*., 2005).

Further, dual color image watermarking caters a coherent way out to two major security concerns: Information recovery and ownership identification. In parliamentary law to resolve ownership authentication any unique attribute like fingerprint, retina scans or DNA structure can be utilized as primary watermark. The secondary watermark may be any user precise essential information. To elevate the auspices level and robustness of the embedded watermark the watermark data are randomized by improved Arnold transform. The hectic transposed secondary watermark is rooted into the primary watermark and the resultant watermark is embedded into the host image. Now the watermarked image may transmit to the destination. During the process of transition it may, subject to different attacks and transmission noises. An effectual digital image watermarking should convince the basic requirement as watermark robustness, embedding competence, image imperceptibility, uniqueness and least computational load for embedding or extracting the watermark (Song *et al*., 2012).

In this the functioning of digital image watermarking scheme is evaluated by employing first three criteria. With regards to invisibility the watermarked image must be indistinguishable from the original. Robust watermarking systems are necessitated to protest different types of

Corresponding Author: A. Lakshmi Priya, Department of ECE, Global Institute of Engineering and Technology, Vellore, Tamil Nadu, India

attacks like image compression, noising, filtering, rescaling, cropping, rotating, etc. At last related to capacity the watermarking system may set out from a low fraction of the host image size to multiple times of the size. Any image watermarking system should balance the right combination of all these measures to attain suitable outcomes.

The majority of researchers is getting along in the field of watermarking is to amend the imperceptibility and robustness. In this study, a novel dual watermarking technique is proposed by utilizing the advantages of multiple transformation techniques like DWT, DCT and SVD (Lakshmi and Letitia, 2015). Consequently the host image is decomposed by three level DWT and then DCT and SVD's are applied to the LL sub band. Now the primary and hectic transposed secondary watermarks embedded image is rooted in it. The experimental result shows that this proposed scheme indulges the demands of digital image watermarking. In the origin procedure, foremost the primary watermark is extracted and compared with its original image based on similarity measures. If the similarity measure meets the specified threshold, then the secondary watermark extraction process is done.

MATERIALS AND METHODS

Discrete Wavelet Transform (DWT): Due to the good energy compaction property of wavelet transform, it becomes an important tool in image processing and watermarking. Many research works in this area took out numerous algorithms to produce efficient wavelets. The DWT separates an image into four regions, lower resolution approximation component (LL) is taken by low pass filtering both rows and columns and contains a fierce depiction of an image, diagonal (HH) component comprises a high frequency component along the slashes. Horizontal (HL) and Vertical (LH) is mid frequencies obtained by low pass filtering in one charge and high pass filtering in another way. The big amount of energy is concentrated in LL sub bands and so embedding in the LL sub band increases the validity of the watermark significantly. Hence, in this algorithm LL is chosen for embedding processing (Naderahmadian and Khayat, 2010; Ali *et al*., 2013).

Discrete Cosine Transform (DCT): DCT is one of the most fascinating linear transformation techniques in signal and image processing. The DCT embeds the watermark in perceptually significant segment of the image is more advantageous because, the compression algorithm only removes the insignificant segment of the image. DCT is mainly chosen because it has semantically meaningful watermark pattern, good perceptual invisibility, adequate robustness, reasonable complexity and implementation time. The 2D discrete cosine transform and its inverse transforms are mathematically represented as:

$$F(k,l)=\frac{2}{\sqrt{N}}a(k)a(l)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(m,n)\cos\left\{\frac{(2m+1)k\pi}{2N}\right\}\cos\left\{\frac{(2n+1)l\pi}{2N}\right\}$$

$$f(m,n)=\frac{2}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}a(k)a(l)F(k,l)\cos\left\{\frac{(2m+1)k\pi}{2N}\right\}\cos\left\{\frac{(2n+1)l\pi}{2N}\right\}$$

Where:

f (m,n) = Pixel representation in the spatial domain

F (k,l) = Its DCT coefficient, m and n represents the block size (Sverdlov *et al*., 2005, 2006).

$$a(k)a(l)=\begin{cases}\frac{1}{\sqrt{2}} & \text{if } u,v=0\\ 1 & \text{else}\end{cases}$$

Singular Value Decomposition (SVD): SVD is a linear algebraic transformation technique which is used in watermarking; it modifies the singular values of the entire host image by embedding the watermark data. The singular value specifies the brightness value of an icon and the singular vector specifies the geometry of the image layer. The robustness of an image is increased by applying SVD because due to attacks, there is a large change in the image which results in a very small change in watermarks. Let S denotes the material matrix of order m×n. The SVD of S in denoted as, $s = u\sigma v^T$ Where ó is the diagonal matrix, u and v are orthogonal matrixes. SVD has fascinating properties: the transformation applied to an image may have an arbitrary size which is not restricted to square image. And the singular value of image posses the intrinsic algebraic property of the image (Liu and Tan, 2002).

Arnold transform: To enhance the security of the watermarking scheme the watermarks are randomized using scrambling before embedding into cover image. Here an improved Arnold transforms is preferred for scrambling. Traditional arnold transforms is defined as:

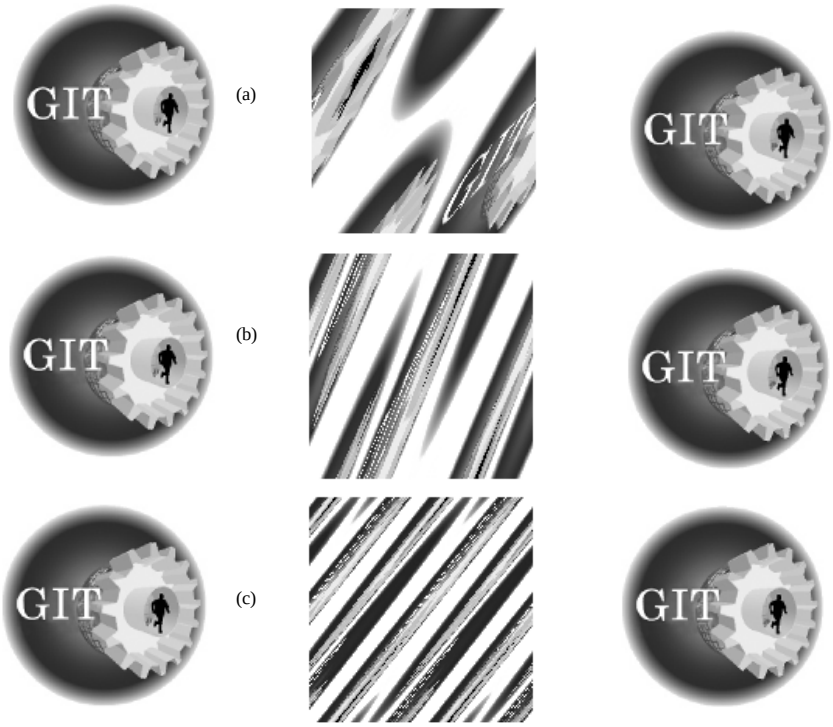

Fig. 1: Arnold transformed and inverse images: a) Original image; b) Arnold transformed; c) Inverse arnold transformed

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

x, y and x_i, y_i are original and transformed images respectively. In this formal method of Arnold transform all the four transform coefficients are fixed hence any one can descramble the image well. Hence block location scrambling algorithm of digital image based on Arnold transform is applied to defeat the above said drawback. The transformed algorithm of this method is given as:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

This should satisfy the criteria ad-bc = 1. Farther out of four matrix coefficients only two are known again limits the selection of choosing different matrix coefficients. These drawbacks are overcome by Improved Arnold Transform is proposed in 2010 by MA DING and FAN JING is given as:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + K \begin{bmatrix} N \\ N \end{bmatrix} \bmod N$$

Where $a_{00} \times a_{11} + a_{01} \times a_{10} = \pm 1$, K = max[ABS($a_{00}$), ABS($a_{11}$), ABS($a_{10}$) ABS($a_{01}$)] and N defines the size of the target image which determines the period of Arnold transform. In this improved Arnold transform all four matrix coefficients are different, thus we can pull in multiple choices among them; so it is hard for the attackers to acquire the original content of the picture. Figure 1 presents a comparison between Traditional, Block location scrambling and Improved Arnold transformed and its opposite. Among which we can find the scrambling factor of improved Arnold transform is very high compared with others (Yin *et al*., 2007; Subramanyan *et al*., 2011).

Proposed algorithm: In this proposed method, the above mentioned algorithms are combined for encrypting and decrypting the image. The detail block diagram is shown in Fig. 2. The original watermark is Arnold transformed different number of times first; discrete wavelet transformed and discrete cosine transformed next. Then the transformed result is decomposed to obtain U, S and V parts using Singular Value Decomposition. This is embedded into the primary watermark to increase the robustness. The new watermarked image is embedded into Host image, yield a watermarked image. The decryption process is explained in Fig. 3. The watermarked image is

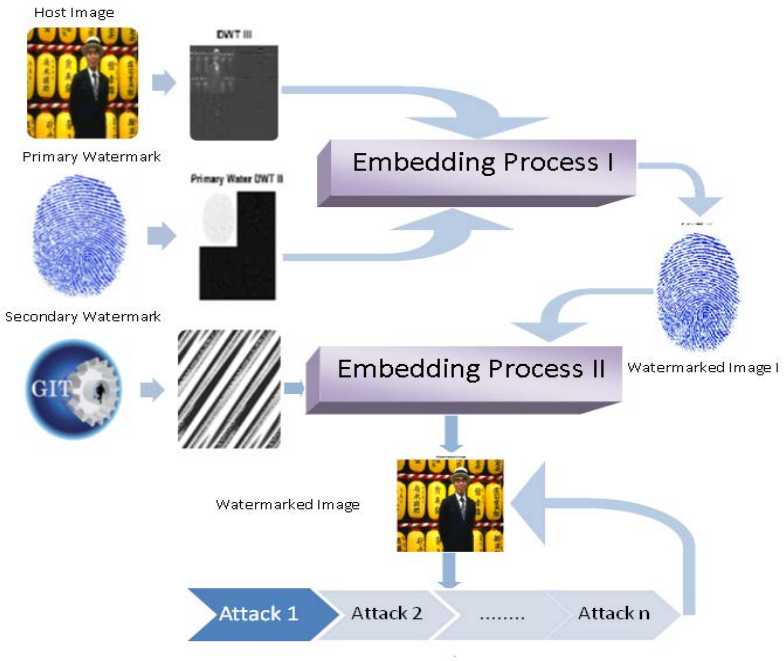

Fig. 2: Embedding tecnique

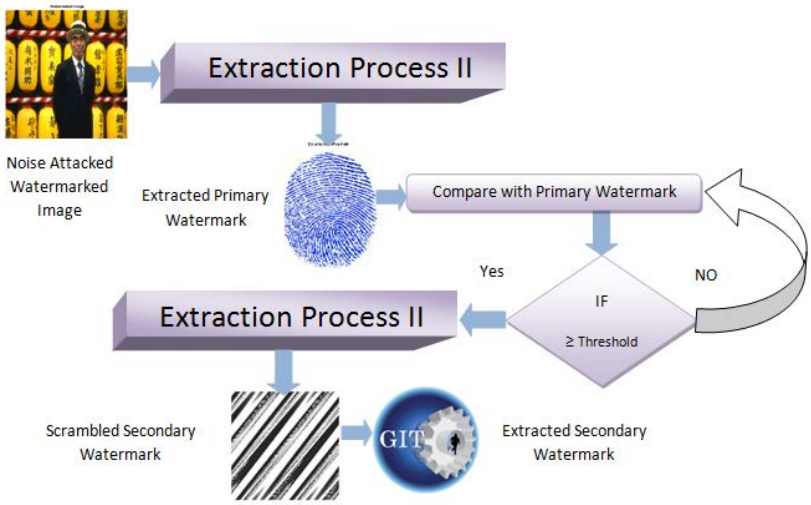

Fig. 3: Extraction process

decrypted by taking discrete wavelet transform, discrete cosine transform and singular value decomposition. All SVD parts of primary watermark are gathered back without missing anyone, where the ownership authentication is verified, if it meets the desired threshold it is decomposed to obtain the secondary watermark.

Embedding procedure: The 3D original color watermark is divided into 2D component watermarks as W_{R2}, W_{G2} and W_{B2}, corresponding to R, G and B components respectively. Each component watermark is permuted by Arnold transform in order to enhance the security and decomposed into U, S and V parts. The primary watermark and the Host image are also divided into three components W_{R2}, $W_{G2,}$ W_{B2} and H_{R}, $H_{G,}$ H_{B} respectively. The blue components are selected and transformed by 3 levels DWT; decompose W_{B2} and H_{B} into LL, LH, HL and HH sub bands and DCT is applied to all Apply SVD partition these values into u, s and v:

$$S^{i} = u_i s_i v_i^T$$

$$i = H_B, W_{B1} \text{and} W_{B2}$$

where, H_B represents the singular values of host image W_{B1} and W_{B2} are the singular values of primary and secondary watermark. Modify the singular values of the diagonal matrix as:

$$s_i^{'} = s_{B1} + \alpha s_{B2}$$

$$s_i^{''} = s_1 + a s_i^{'} \overset{\text{Inverse}}{\Leftrightarrow} u_k^{'} s_k^{'} v_k^T$$

$S^{''}$ represents the new singular value obtained from host and watermarks. Then apply inverse DCT and inverse DWT to obtain the watermarked image. Figure 2 represents the Embedding process where the Host image and Watermarks are embedded.

Extraction procedure: The watermarked image work is decomposed by applying 3 levels DWT, DCT and then SVD. Extract the singular value matrix $S^{''}_{wk}$ of the watermarked image W_k:

$$S^{''}_{wk} = \left(S'_{wk} - S^{*}_{wk}\right) / \alpha$$

Where:

S^{*}_{wk} = Diagonal matrix of Watermarked image
$S^{''}_{wk}$ = Diagonal matrix of Extracted Watermark
α = Scaling factor

From $S^{''}_{wk}$ segregate the singular values and compute inverse SVD, DCT and DWT to obtain primary watermark. Singular values of secondary watermarks are extracted from primary watermark and inverse Arnold transformed. Figure 3 represents the extraction algorithm which retrieves the watermark images back after attempting with all feasible attacks.

RESULTS AND DISCUSSION

In the following experiments, 24 bit color image with a size of 512 x 512 is selected as the host image. Two 24 bit color images of the same size are chosen as primary and secondary watermarks, shown in Fig.4a-c respectively. The imperceptible and robustness capability of the watermark is investigated by measuring peak signal to noise ratio and normalized correlation. Peak signal to noise ratio is employed to evaluate the difference between the original and a watermark signal to noise ratio is employed to evaluate the difference between the original and watermark image shown in Eq. 1. For robustness normalized correlation measures the similarities between the original and watermark image shown in Eq. 2. The larger PSNR and higher NC reveal the extracted watermark resemble the original watermark:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x(i,j) - W_K^{*}(i,j)\right)^2$$

$$PSNR = 10\log 10\left(\frac{255^2}{MSE}\right)$$

and:

$$NC = \frac{\sum_i^m \sum_j^n \left[x(i,j) w_k^{*}(i,j)\right]}{\sqrt{\sum_i^m \sum_j^n (x(i,j))^2} \sqrt{\sum_i^m \sum_j^n (w_k^{*}(i,j))^2}}$$

The invisibility of the watermark is evaluated by embedding the watermark in the host image as shown in Fig. 5. The obtained PSNR and NC value shows that better visual quality of watermarked image is obtained by the proposed algorithm. The higher NC designates that extracted watermark resembles the original watermark shown in Fig. 6. In following, various attacks such as JPEG, Cropping, adding noise, rotation, filtering, scaling, blurring, smoothening etc., are performed to investigate the robustness of the watermarked image. The attacks aim to remove the watermark without breaking the security of the watermarking algorithm is referred as removal attacks. Noising, histogram equalization, sharpening, compression and blur are included in this category. Instead of removing the watermark certain attacks intends to distort it such attacks are acknowledged as geometrical attacks which includes rotation, scaling, cropping, warping, recycling, etc. The process used for correcting this type of attacks is referred as synchronization. Cryptographic, protocol attacks are used to identify the algorithm used in the watermarking scheme and targets the entire concept of watermarking respectively. Brute-force search method and copy attacks are few lies in the category. The main objective of the proposed algorithm affects only on the removal and geometric attacks. By understanding the concepts one could identify the similarities in effects between different attacks and also device a way out to alleviate the effects on existing technique.

Fig. 4: a) Host image; b) Primary watermark; c) Secondary watermark

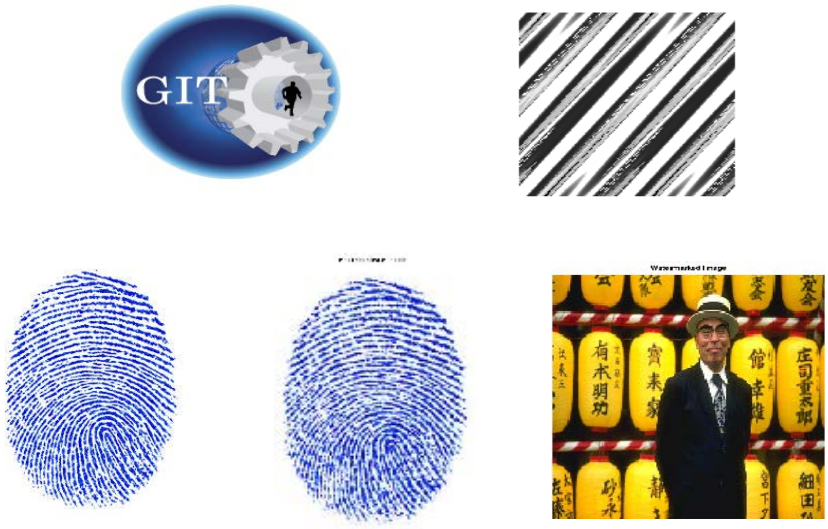

Fig. 5 a) Secondary Watermark; b) Scrambled secondary watermark; c) Primary watermark; d) Secondary embedded primary watermarked image; e) Watermarked Image with PSNR and NC

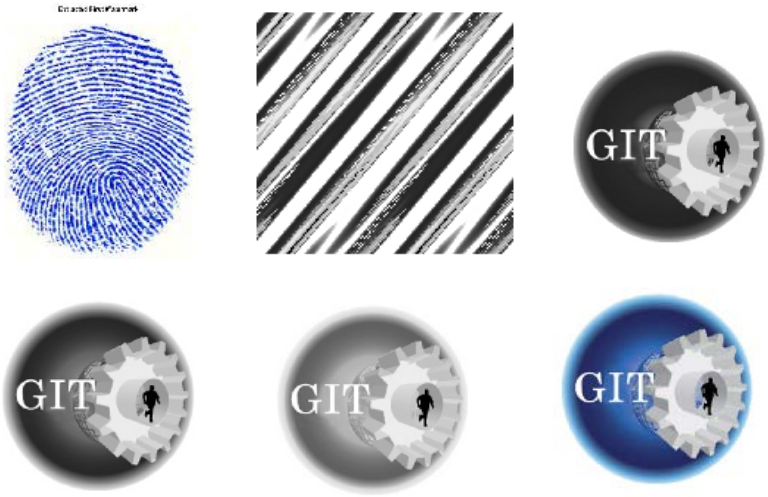

Fig. 6: a) Extracted Primary Watermark with PSNR and NC values; (b) Extracted Scrambled secondary watermark; cde) R,G and B components of Extracted secondary watermark; f) Extracted secondary Watermark with PSNR and NC

Removal attacks: Removal attacks include; adding noise like Salt and Pepper noise, Gaussian noise, Speckle noise, Poisson noise, Motion blurring, Sharpening, filtering like a Median filter, average filter, JPEG compression,

Fig. 7: a) Salt and pepper noised image with s = 0.1; b) Extracted primary watermark with NC = 0.9849; c) Extracted krmark with N C = 0.9585

Fig. 8: a) Histogram equalized watermarked image; b)Extracted primary watermark with NC = 0.9987; c) extracted secondary watermark with NC = 0.9707

Fig.. 9: a) The 70% compressed watermarked image; b) Extracted primary watermark with NC = 0.9959; c) Extracted secondary watermark with NC = 0.8728

Histogram equalization and contrast adjustment. Salt and pepper noise is typically seen on the images. It is sparsely occurring as white and black pixels. The noising scheme generates 1-15% to degrade the quality of the watermark. Gaussian noise is a statistical noise having a probability density function equal to a Gaussian distribution, caused by poor illumination, high temperature and from many natural sources. By adding such noises deliberately corrupts the watermarked image and reduces its visual quality. The mean of the Gaussian function is varied from 1-30% in order to examine the robustness of the proposed method. Speckle and Poisson noises are also generated in a similar way to check the trustworthiness of watermarked image. Histogram equalization works by reducing the number of unique gray levels to approximate a uniform distribution. Sharpening amplifies the presence of edges in an image. JPEG compression produces artifacts on the compressed image which allows JPEG to attack watermarks. Figure 7-15 shows some of the watermarked image affected by Removal attacks and the extracted watermark.

Geometry attacks: Geometry attacks are different from removal attack which includes, Rotating at various angles, Cropping or deleting rows or columns, rescaling that is reducing the size of the image to 75% and Warping. Figure 16-19 shows the geometry attack affected watermarked image and the extracted watermark with NC values. Figure 20 shows the comparison in terms of NC values for different attacks by varying its parameter. The graph shows both primary and secondary watermarks are extracted with better quality.

The proposed watermarking scheme is robust to many attacks. It also observed the proposed method provides better result in all the cases, both watermarks are obtained equally good. Figure 21 illustrates the best

Fig. 10: a)Poison noised watermarked image; b)Extracted primary watermark with NC = 0.9999; c) Extracted secondary Watermark with NC = 0.8549

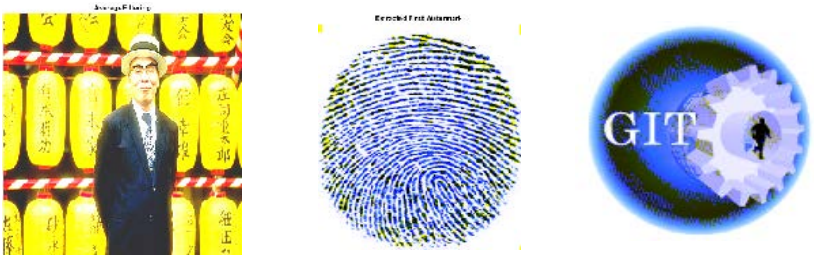

Fig. 11: a)Averaging filtered Watermarked Image; b)Extracted primary watermark with NC = 0.9773; c) Extracted secondary Watermark with NC = 0.9710

Fig.12: a)Median filtered Watermarked Image; b)Extracted primary watermark with NC = 0.9437 ; c) Extracted secondary Watermark with NC = 0.8122

Fig. 13: a)Edge Sharpened Watermarked Image; b)Extracted primary watermark with NC = 0.9875; c) Extracted secondary Watermark with NC = 0.9497

among different NC values of the extracted watermark under different attacks by the proposed algorithm. From Fig. 21 the proposed algorithm gives better result for the primary watermark and however the secondary watermarks NC values are slightly lower than the primary. In all cases the NC values of the primary watermark meet the desired threshold.

Fig. 14: a) Blurred watermarked Image; b)Extracted primary watermark with NC = 0.9875; c) Extracted secondary watermark with NC=0.9497

Fig. 15: a) Gaussian Noise added watermarked image; b)Extracted primary watermark with NC = 0.9980; c) Extracted secondary Watermark with NC = 0.9701

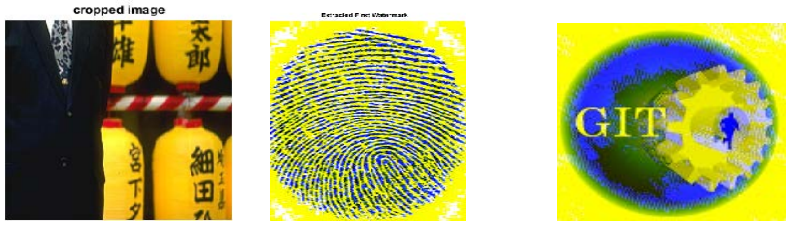

Fig.16: a) Cropped watermarked image250x250; b)Extracted primary watermark with NC = 0.8478; c) Extracted secondary Watermark with NC = 0.8007

Fig.17: a) Rotated watermarked image at 20; b) Extracted primary watermark with NC = 0.7888; c) Extracted secondary watermark with NC = 0.8188

Fig. 18: a) Rescaled by [384 384]:0.75; b)Extracted primary watermark with NC = 0.9997; c) Extracted secondary Watermark with NC = 0.8778

Fig. 19: a) Warped watermarked image; b) Extracted primary watermark with NC = 0.9999; c) Extracted secondary Watermark with NC = 0.8549

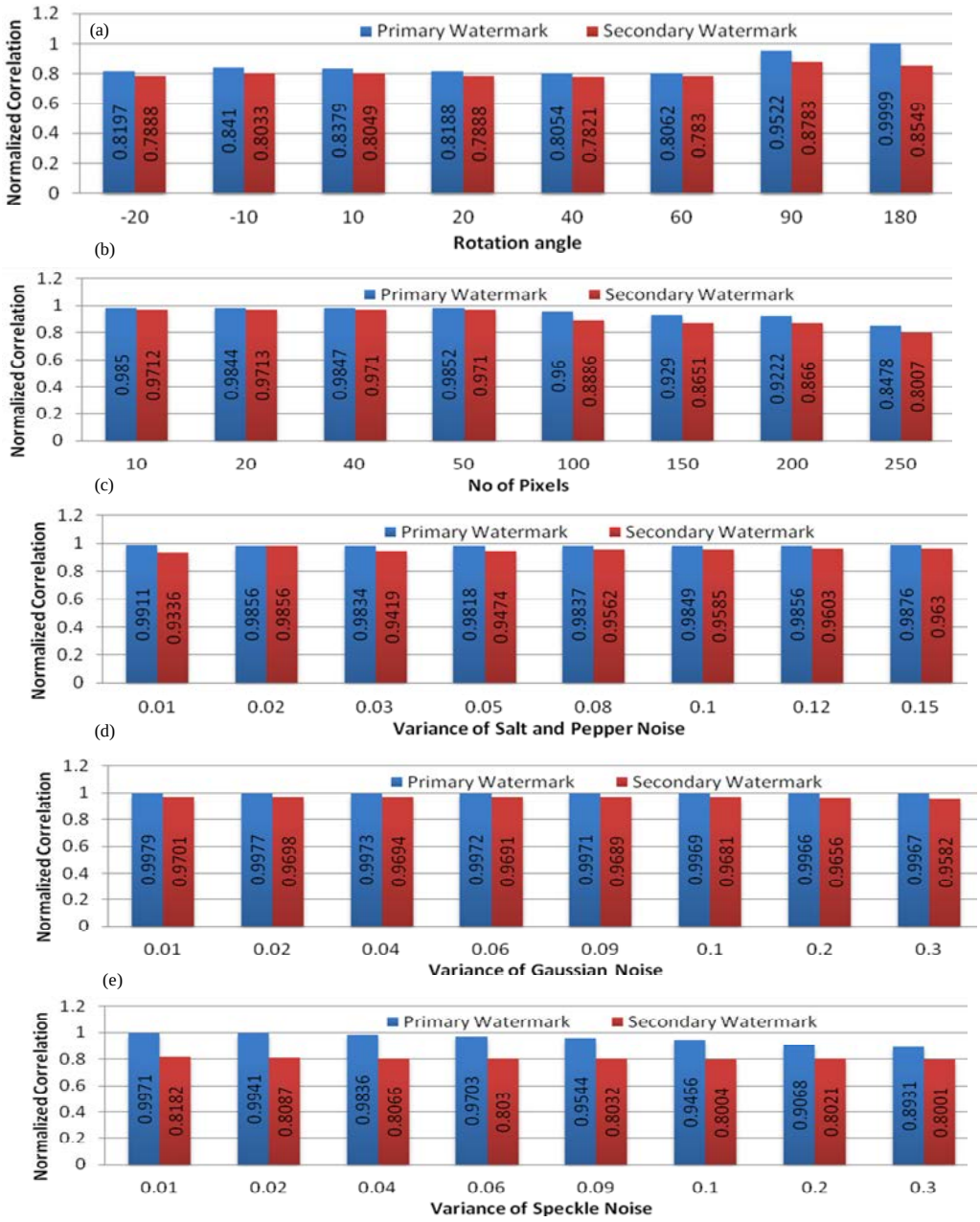

Fig. 20: Continue

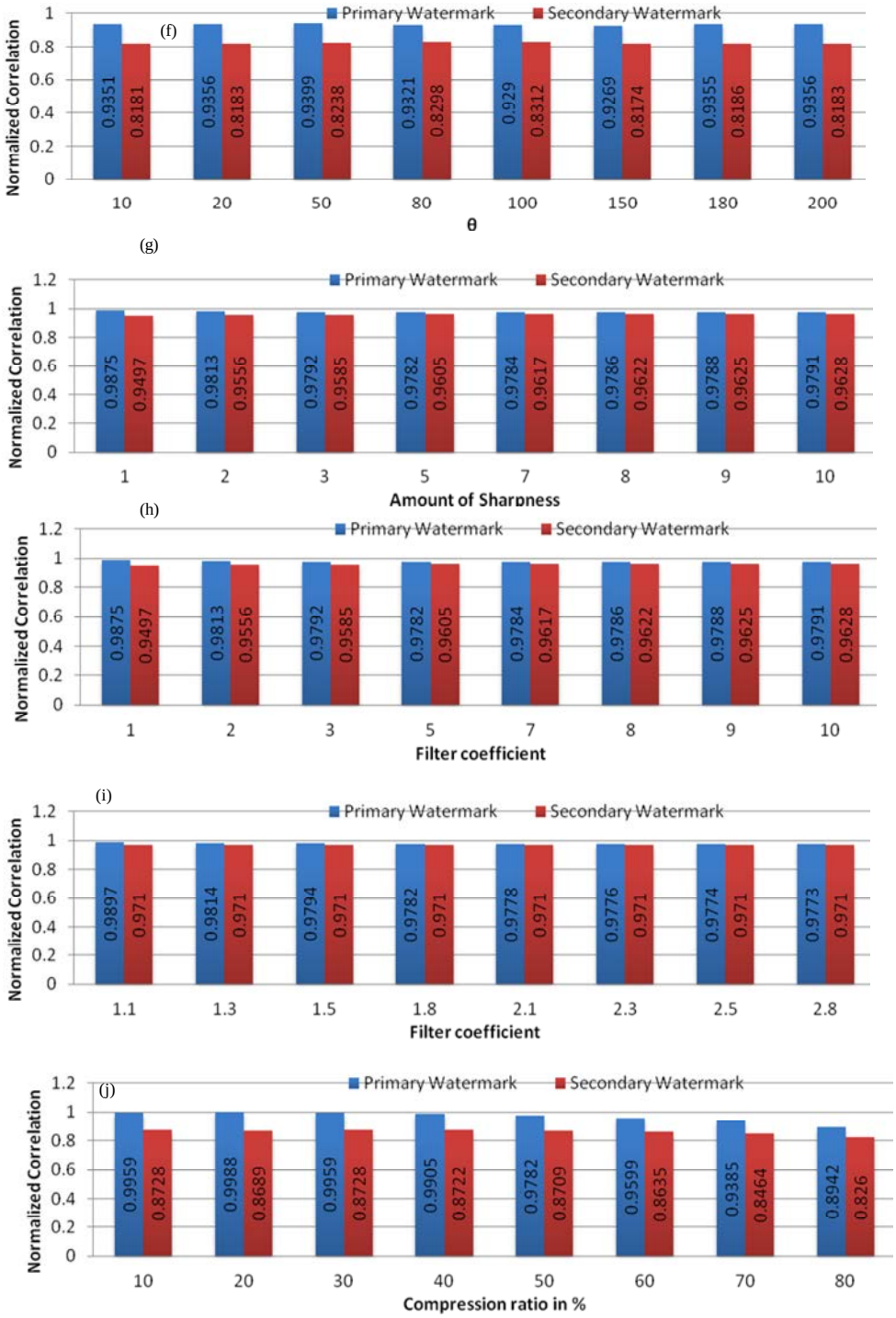

Fig. 20: a) Comparison of different values of parameter of different attacks; a) Comparison by varying the rotating angle; b) Comparison by varying number of pixels; c) Comparison by varying the variance of salt and pepper noise; d) Comparison by varying the variance of gaussian noise; e) Comparison by varying the variance of speckle noise; f). Comparison by varying θ with constant ln of motion blur; g) Comparison by varying the sharpness level; h) Comparison by changing the order of median filter; i) Comparison by varying the filter coefficient of average filter; j) Cjanuary 4, 2017omparison by varying the compression ration

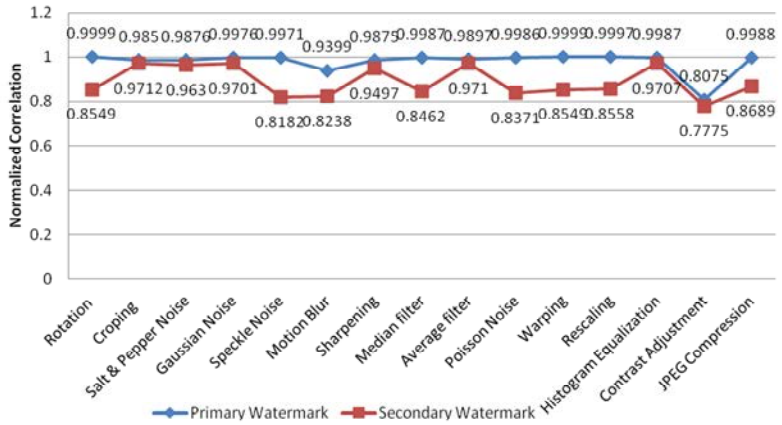

Fig. 21:Comparision of algorithm in terms of its best NC values

CONCLUSION

A novel robust and efficient dual watermarking scheme is proposed in this paper. The most significant feature is to use improved Arnold to enhance the invisibility and robustness. It successfully embeds primary and secondary watermarks with best PSNR and NC. At first the primary watermark is extracted with good quality and greater threshold. Hence the randomized secondary watermark is extracted back. By properly choosing the coefficients of Arnold the original secondary watermark is extracted with best NC values after attempting all sorts of possible attacks. The experimental results shown in this algorithm not only guarantees the invisibility, but also has a strong robustness on different image processing attacks. In future, the invisibility of the watermark with larger threshold is to be considered and also the same may be attempted in video images too.

REFERENCES

Ali, M., C.W. Ahn and M. Pant, 2013. An optimized watermarking technique based on DE in DWT-SVD domain. Proceedings of the 2013 IEEE Symposium on Differential Evolution (SDE), April 16-19, 2013, IEEE, New York, USA., ISBN:978-1-4673-5873-6, pp: 99-104.

Jia, S.L., 2014. A novel blind color images watermarking based on SVD. Opt. Intl. J. Light Electron Opt., 125: 2868-2874.

Lakshmi, P. and S.A. Letitia, 2015. Copyright protection for digital colour images in RGB planes using improved DWT-DCT-SVD algorithm. Intl. J. Appl. Res., 10: 42815-42821.

Liu, R. and T. Tan, 2002. An SVD-Based watermarking scheme for protecting rightful ownership. IEEE Trans. Multimedia, 4: 121-128.

Naderahmadian, Y. and H.S. Khayat, 2010. Fast watermarking based on QR decomposition in wavelet domain. Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), October 15-17, 2010, IEEE, New York, USA., ISBN:978-1-4244-8378-5, pp: 127-130.

Potdar, V.M., S. Han and E. Chang, 2005. A survey of digital image watermarking techniques. Proceedings of the 3rd International Conference on Industrial Informatics, August 10-12, 2005, IEEE, pp: 709-716.

Song, C., S. Sudirman and M. Merabti, 2012. A robust region-adaptive dual image watermarking technique. J. Visual Commun. Image Represent., 23: 549-568.

Subramanyan, B., V.M. Chhabria and T.S. Babu, 2011. Image encryption based on AES key expansion. Proceedings of the 2011 2nd International Conference on Emerging Applications of Information Technology (EAIT), February 19-20, 2011, IEEE, New York, USA., ISBN:978-1-4244-9683-9, pp: 217-220.

Sverdlov, A., S. Dexter and A.M. Eskicioglu, 2005. Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies. Proceedings of the 2005 13th European Conference on Signal Processing, September 4-8, 2005, IEEE, New York, USA., ISBN:978-160-4238-21-1, pp: 1-4.

Sverdlov, A., S. Dexter and A.M. Eskicioglu, 2006. Secure DCT-SVD domain image watermarking: Embedding data in all frequencies. Department of Computer and Information Science, Brooklyn College, City University New York, New York, USA.

Yin, C.Q., L. Li, A.Q. Lv and L. Qu, 2007. Color image watermarking algorithm based on DWT-SVD. Proceeding of the IEEE International Conference on Automation and Logistiocs, August 18-21, 2007, Jinan, China, pp: 2607-2611.